HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Découverte de réseaux IPv6

Nicolas Collignon
<Nicolas.Collignon@hsc.fr>

Au programme

- Rapide rappel sur IPv6
- Concepts
- Optimisations
- Introduction au framework ***sherlock***
- Implémentation de ***sherlock-net***

Petit rappel sur IPv6

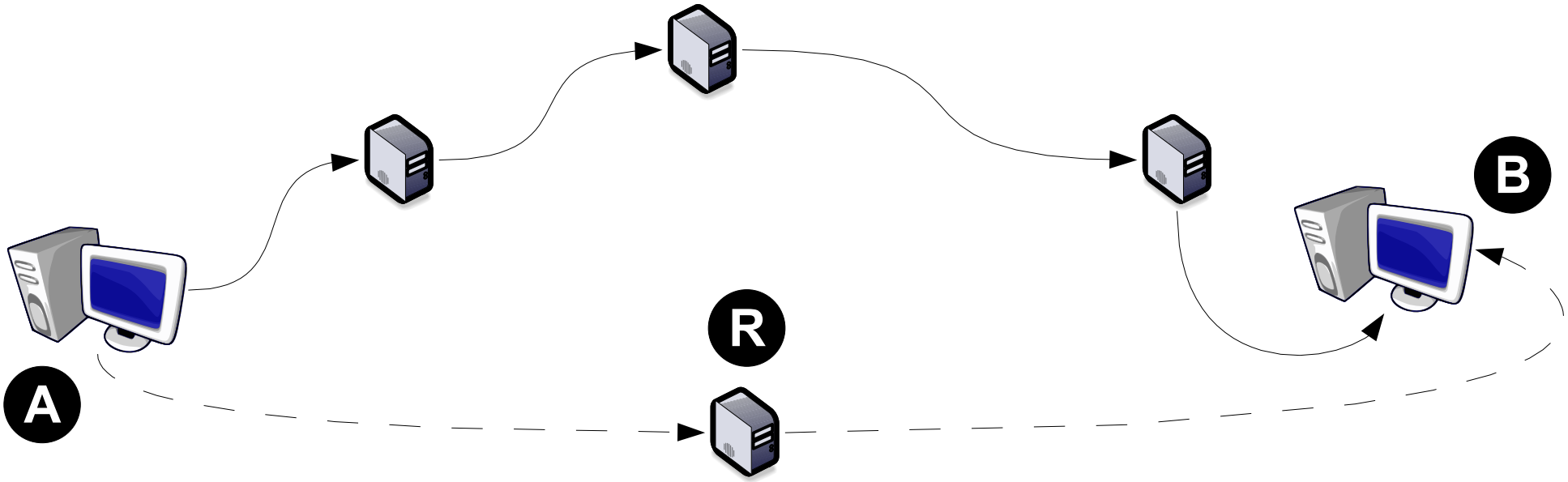
- Protocole encore faiblement utilisé
- Énorme espace d'adressage
- Réseaux moyens : **2^{80}** à **2^{96}** adresses 
- Différents périmètres d'adresses
- Options IPv4 ► Extensions IPv6

Périmètres d'adresses

- IPv4
  - Adresses Publiques ► Internet IPv4
  - Adresses Privées
- IPv6
  - Périmètre global ► Internet IPv6
  - Périmètre restreint :
    - Node-Local
    - Link-Local
    - Site-Local

Les en-têtes de routage de type 0

- IPv4 « source routing » ► RH Type 0
- Permet de spécifier une liste de *hops* intermédiaires
- L'adresse de destination change à chaque *hop*



Concepts

- Scan sur le lien
- Scan distant
- Détection distante des adresses non-routables

Scan sur le lien

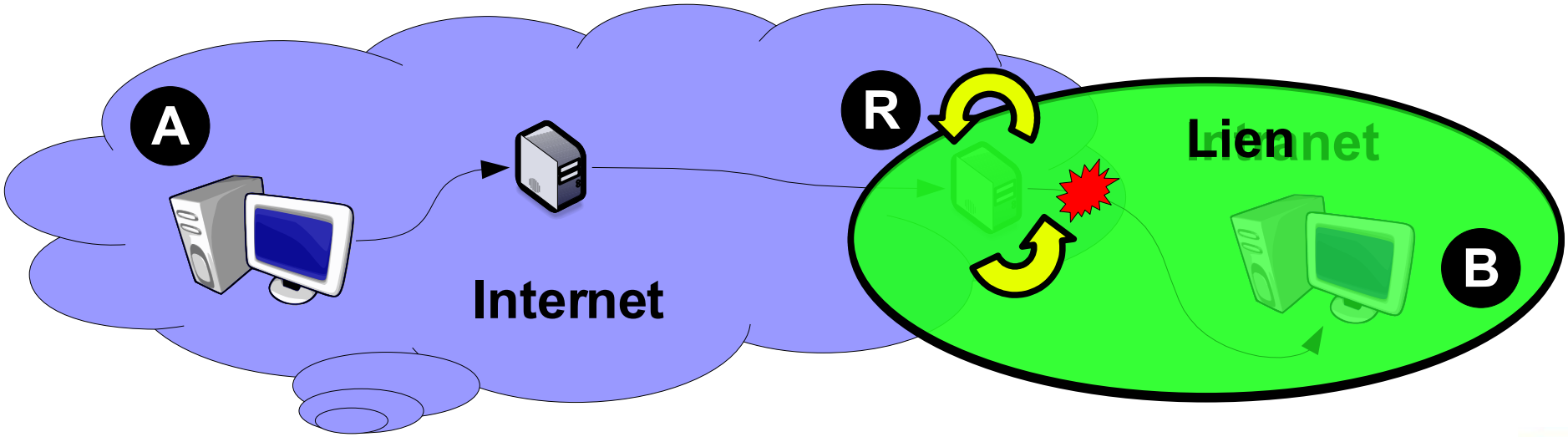
- Principes équivalents à IPv4
  - Nécessite une résolution d'adresses couche OSI 3 ► 2
  - Équivalent d'un scan ARP who-has
- NDP basé sur ICMPv6
  - Interrogation de l'adresse Multicast all-nodes **`ff02::1`**
  - **Neighbor Solicitation** / **Neighbor Advertisement**
- Interrogation des Multicasts
  - Utilisation plus forte des Multicasts avec IPv6
  - Source d'information rapide

Scan distant

- Principes équivalents à IPv4
- Protocoles avec états
  - ex: TCP, ICMPv6, SCTP
- Protocoles sans état niveau couche OSI 4
  - ex: UDP
  - Implique la réception des paquets ICMP **Port Unreachable**
- Protocoles sans état niveau couche OSI 5+
  - ex: SNMP, DNS, NTP
  - Implique le support des protocoles applicatifs associés

Scan d'adresses non routables

- À oublier « *grâce* » aux récents évènements
- Pas de vérification du périmètre des adresses des *hops*
  - Détection des adresses de périmètre non-global à distance
- Permet de contacter des réseaux non routés



Les « modèles » d'adressage

- Modèle générique des architectures
  - Adressage par location
  - Adressage par utilisation ► serveurs, pare-feu, stations de travail ...
- Modèles « simples » d'adressage IPv4
  - 1 adresse par interface réseau sauf sur les passerelles
- Modèles « hybrides » d'adressage IPv6
  - N adresses par interface réseau (N >= 2)
  - moins de maîtrise sur l'adressage
    - Adressage mixte : statique et dynamique
    - Adressage à périmètre variable

Configuration des adresses IPv6

- Configuration « sans état »
  - Adressage automatique ► EUI-64, CGA
  - Adressage manuel
    - Adressage séquentiel ► suites arithmétiques ou géométrique
    - Motifs ► « `beef` », « `cafe` », « `abcd` » ...
- Configuration « avec état »
  - Adressage séquentiel ► DHCPv6, GGSN
- Adresses temporaires IPv4 ≠ Privacy Extensions IPv6
  - Nécessité d'avoir au moins une autre adresse pour la traçabilité

Comment faciliter le scan ?

- Le service DNS

- Réduction de l'espace d'adressage
  - Adresses EUI-64
  - Adressage « humain »

DNS Mapping

- Requêtes AXFR
- Attaque par dictionnaire
- Structure des noms d'hôte récurrente
- Reverse DNS utiles

www.hsc.fr
www1.hsc.fr
www2.hsc.fr

ftp.hsc.fr
pubftp.hsc.fr

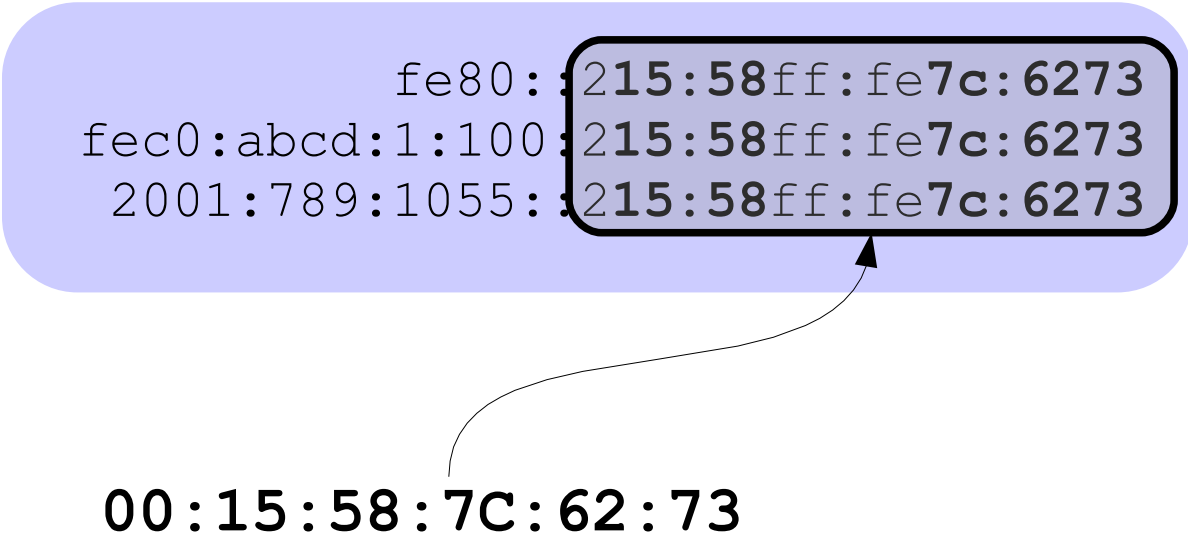
mail.hsc.fr
smtp.hsc.fr
pop.hsc.fr

desk01.hsc.fr
desk02.hsc.fr
desk03.hsc.fr

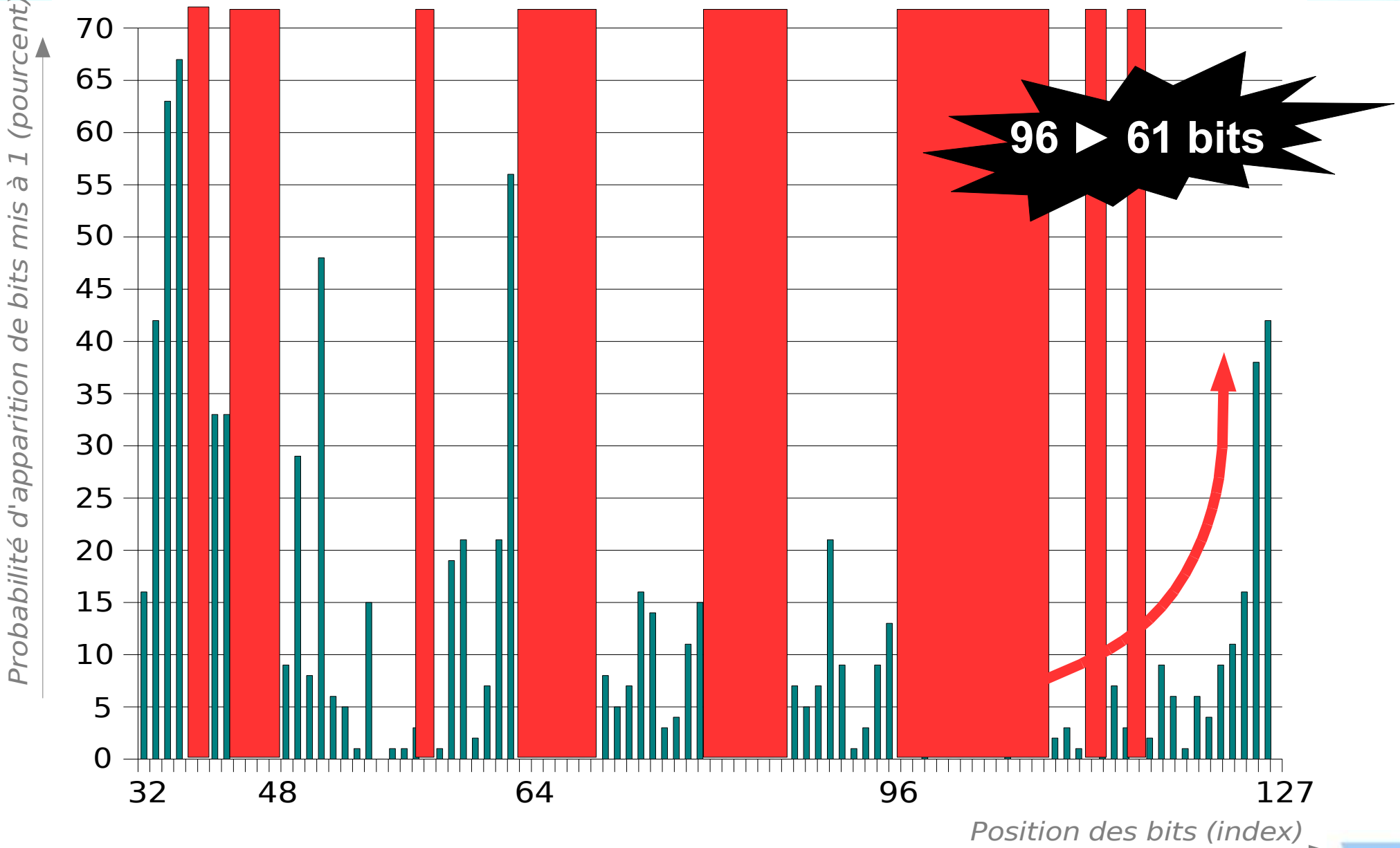
it0-1-1.rev.hsc.fr
it0-1-2.rev.hsc.fr

Les adresses EUI-64

- Génération d'un suffixe de 64 bits avec 48 bits d'information
- Mécanisme d'autoconfiguration utilisé par défaut ► Ethernet
  - Omniprésentes sur les réseaux IPv6
- Utilisé pour les différents périmètres
  - Adresses Link-Local
  - Adresses Site-Local
  - Adresses globales



Statistiques sur les suffixes IPv6 1/2



Statistiques sur les suffixes IPv6 2/2

- Réduction de l'espace d'adressage ► **36 %** 
- **40%** avec 48 bits consécutifs nuls
- **50%** avec 32 bits consécutifs nuls
- **10%** avec les 8 derniers bits nuls
- **<5%** contiennent des lettres ► notation décimale 

sherlock & sherlock-net

Le framework Sherlock

- Objectif : Réalisation de tâches longues et coûteuses
- Modèle réparti N ► 1
- Base générique : gestion des ressources par *plugins*

sherlock-net

- Un mini « *seti@home* » de l'IPv6
- **Pas un botnet** 
  - Modèle réparti pour simplifier l'implémentation
- Utilisation « conseillée » :)
  - Consultants sécurité réseau
    - Scanner un réseau IPv6 dans un laps de temps raisonnable
  - Administrateurs réseaux
    - Évaluer la vitesse de découverte de l'adressage IPv6

L'approche sherlock-net

- Scanner en parallèle
- Scans « intelligents »
  - Gestion de priorités de réalisation
  - Modifier les paramètres d'un scan en fonction de ces résultats
  - Détecter le modèle d'adressage utilisé
- Extraction des informations dans les protocoles applicatifs
  - ex: HTTP, DNS

Support des expressions rationnelles

- Intérêt : Exprimer simplement des tâches réseaux complexes
- Permet :
  - Calcul du coût associé à une expression régulière 
  - Calcul du nombre d'itérations nécessaires pour trouver une information
  - Itération sur toutes les combinaisons possibles
- Syntaxe « maison »

Exemples de commandes sherlock-net

- Traceroute ICMPv4

```
ping -ttl [1-64] 192.168.0.1
```

- Scan de ports TCP

```
tcp -syn -dport * 1664::([0-10]|[100-200])
```

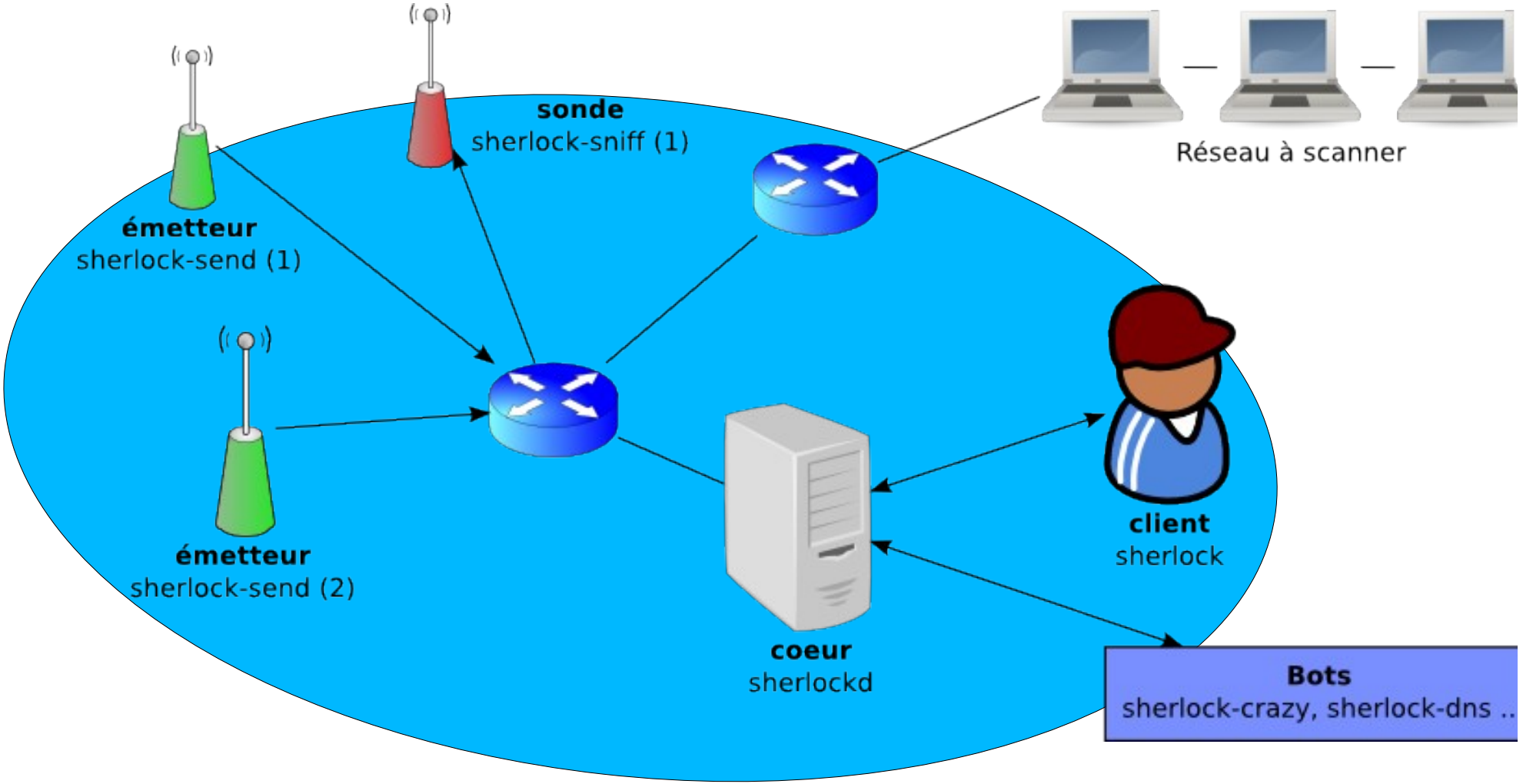
- Bruteforce de nom d'hôte

```
ns_a gw-[0-2].hsc.fr
ns_a @mydict@.hsc.fr
```

- Scan des adresses EUI-64 des équipements Cisco

```
ping fec0:beef::$eui64(cisco)
```

Architecture



Le « cœur »

- Serveur en écoute sur le réseau ou en local
- Intelligence minimale
- Rôles :
  - Répartir les tâches sur plusieurs « *workers* »
  - Journaliser les tâches mises en file d'attente
  - Stocker les informations : adresses, préfixes, noms d'hôtes ...
- Aucune coordination directe entre les sniffers et les émetteurs

L'émetteur

- Injection à niveau variable des paquets
  - Ethernet, IPv6
  - 6in4
- Types de Scans supportés :
  - TCP / SYN
  - UDP / DNS
  - ICMPv6 / Echo Request

bot « crazy »

- **Objectifs**
  - Détecter un motif dans les informations collectées
  - Mettre des tâches « courtes » dans la file d'attente du serveur en fonction des informations collectées
- **Méthodes**
  - Détection des adresses IPv6 EUI-64
  - Détection de numéro de ports dans les adresses IPv6
  - Détection des adresses 6in4
  - Détection de motifs « simples » dans les adresses IPv6
  - Détection de motifs dans les noms d'hôte

bot « bunny »

- **Objectif**
  - Recherche d'adresses valides en se basant sur la taille d'un sous-réseau
  - Ajuster la priorité du scan en fonction de la file d'attente

- **Méthodes**
  - Génère une liste d'adresses en se basant sur des probabilités

bot « bobby »

- **Objectif**
  - Collecter des informations génériques

- **Méthodes**
  - Détermination de la taille des sous-réseaux avec requêtes whois
  - Interrogation des Reverse DNS
  - Traceroute Multiprotocole
  - Prise d'empreinte minimaliste de la pile

TODO... ;)

Option « rendre-malade-les-IDS », Anti-Anti-Sherlock, Ajout aléatoire d'extensions IPv6, Scan à distribution non-uniforme, Fragmentation, Fréquence d'émission, Détection de ta taille des sous-réseaux routés par un routeur, détection des passerelles 6to4, tsp, isatap, Scan sur les adresses link-local et site-local, Option « je-veux-un-joli-schéma » HTML/OpenDocument/SVG, Algorithme génétique pour trouver la meilleur expression régulière d'un bot, Support Scan SNMP, SCTP, MGCP, SIP .., Support des Scan en mode non privilégié : connect, system(« ping »), Support de john, Support de rcrack, Prises d'empreintes des systèmes d'exploitation, Interface GTK click-and-scan, Gestion avancée des droits des clients, Support Windows, Séparation du code en bibliothèques, Documentation avec doxygen, Serveur Web d'administration Python, Scan IPv4, Support client AS/400 :>, Support base de données externes, backend SQL, fonctionnement en mode distribué offline, support rcrack/rtgen, détection du modèle des suites utilisées pour l'adressage (géométrique vs. arithmétique), Plugin NetCraft, Option « audit-da-network » metasploit + autopwn :D, support Windows, scripting Python/Perl/EcmaScript, manpages ...

En bref ...

- Approche non-linéaire du scan
- Les DNS sont très utiles
- « Facile » de découvrir les adresses « simples »
- Permet d'assister au scan
- Disponible sur cvs à la fin de l'année

(en même temps que duke nukem forever)

Merci pour votre attention.

Des questions ?

Nicolas Collignon
<Nicolas.Collignon@hsc.fr>