Source Address Validation Improvements (SAVI)

Mécanismes de prévention contre l'usurpation d'adresses IP source

SSTIC 2012

Orange Labs

Jean-Michel Combes (France Telecom – Orange)

Maryline Laurent (Telecom SudParis)

orange™

sommaire

- Principales attaques
- Network Ingress Filtering
- Limites
- Principes de SAVI
- DHCP SAVI
- FCFS SAVI
- SEND SAVI
- MIX SAVI
- Intégration/Implémentation/Déploiement
- Limites de SAVI
- Potentiels futurs travaux à l'IETF

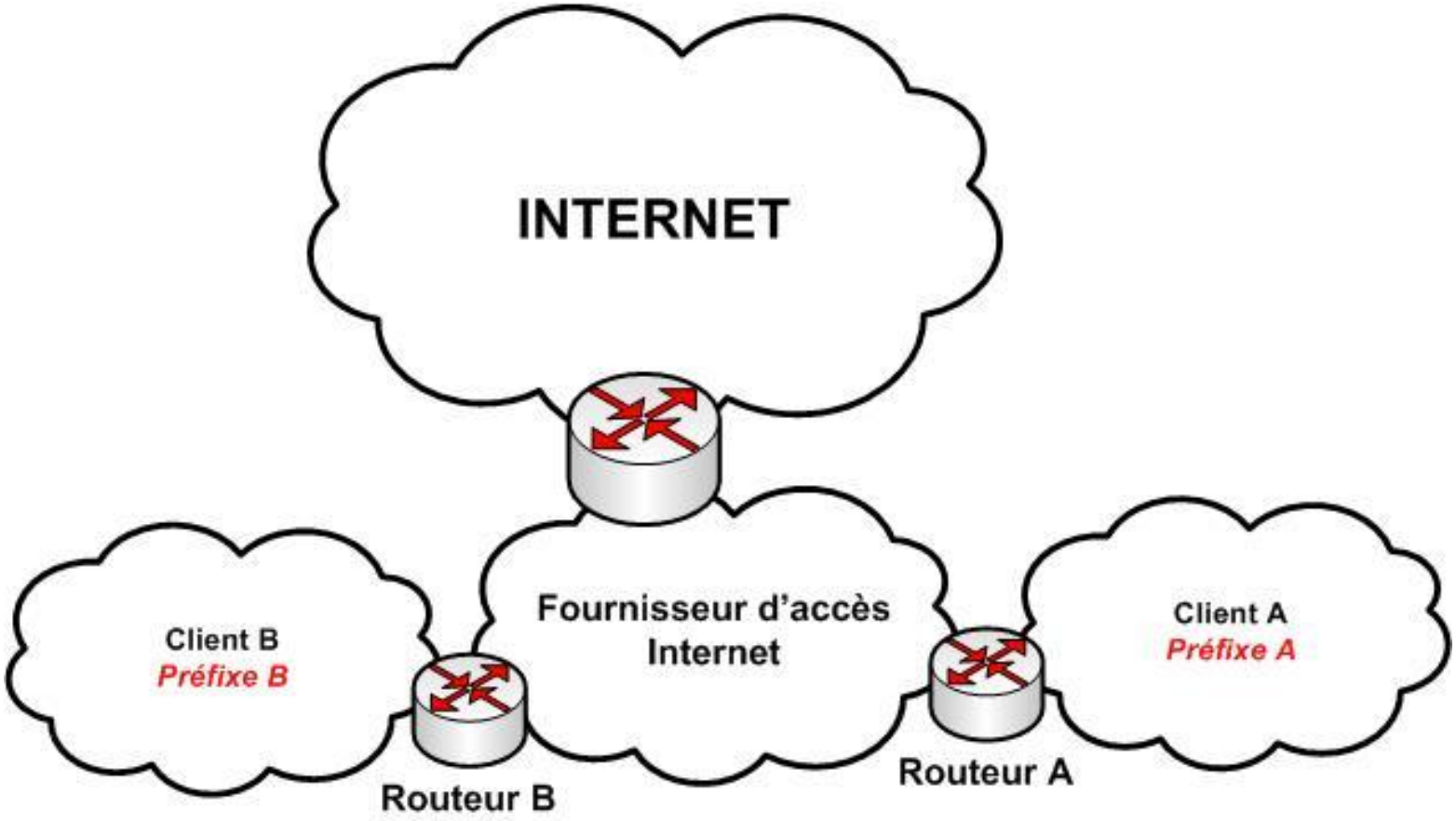
Principales attaques

- Poisoning
  - ARP Poisoning
  - NDP Poisoning (Neighbor Cache, Default Router List, etc.)
  - Table de routage
  - DNS Cache Poisoning
- Denial of Service
  - LAND
  - UDP Flooding
  - TCP SYN Flooding
  - ICMP Flooding
- Reconnaissance & infiltration
  - nmap

Network Ingress Filtering

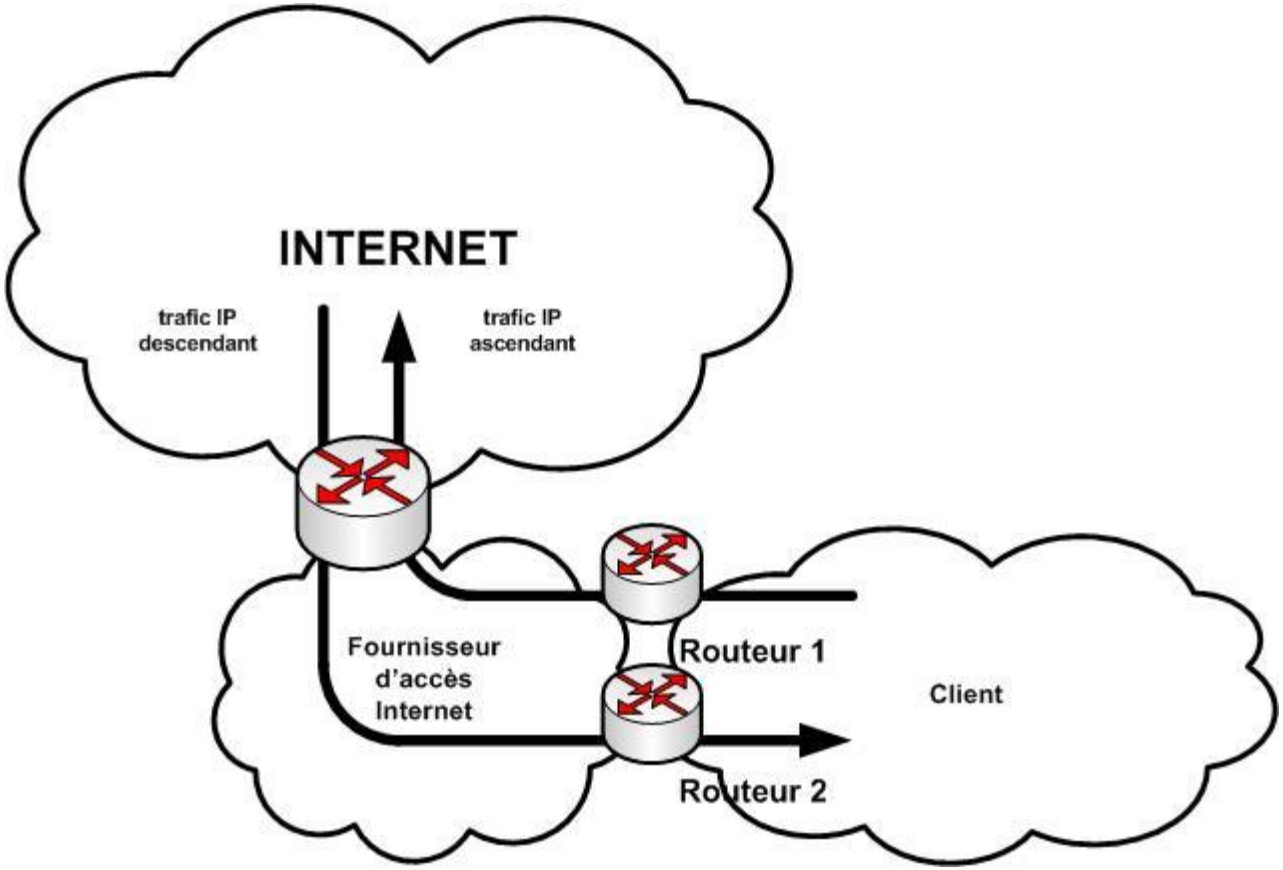
- Augmentation des attaques DoS
- Réaction de l'IETF
  - BCP 38 [RFC2827]
    - Filtrage statique (routeurs)
  - BCP 84 [RFC3704]
    - uRPF
    - Filtrage dynamique (routeurs)
    - Mises à jour basée sur les règles de routage (e.g., BGP)

Network Ingress Filtering



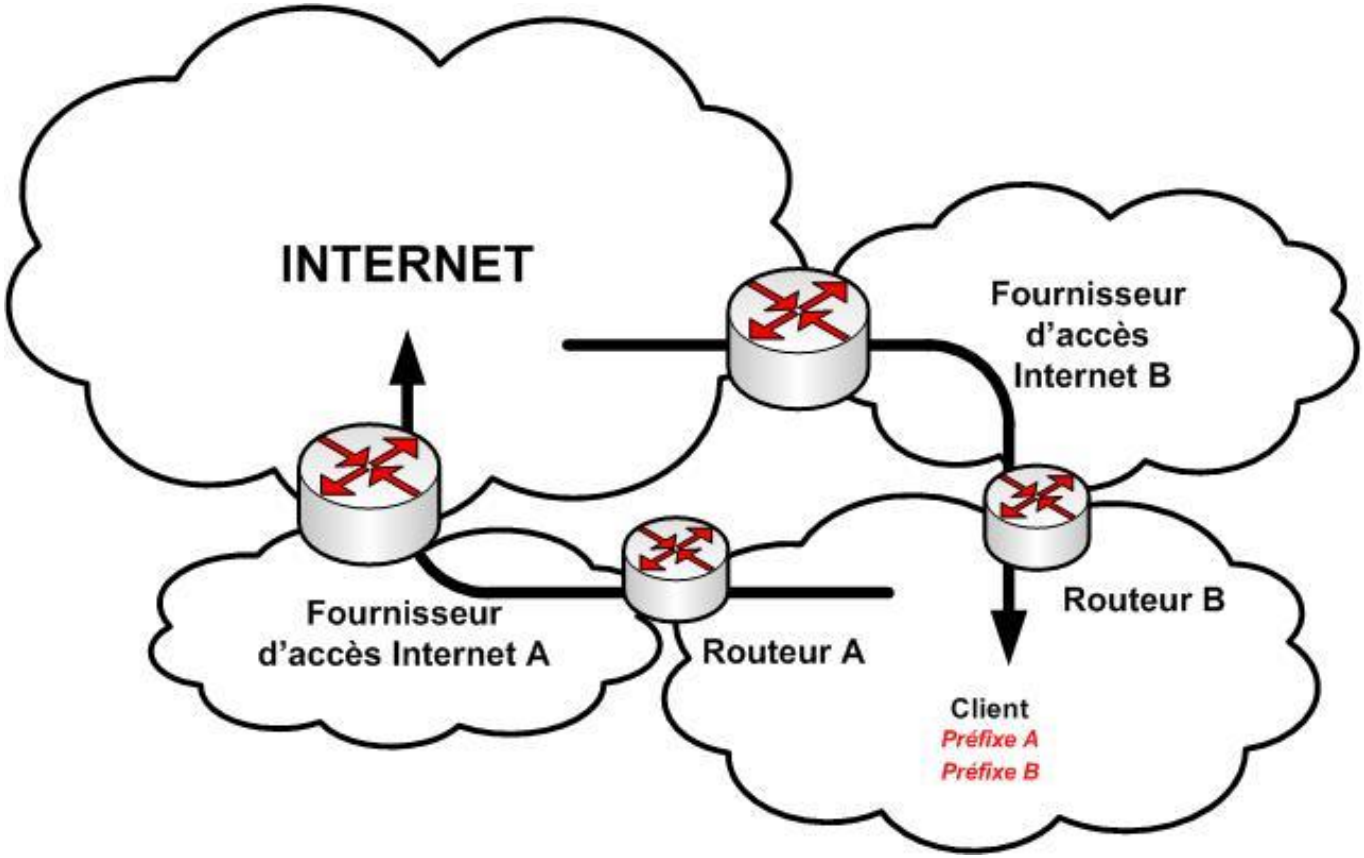
Limites

- Routage asymétrique



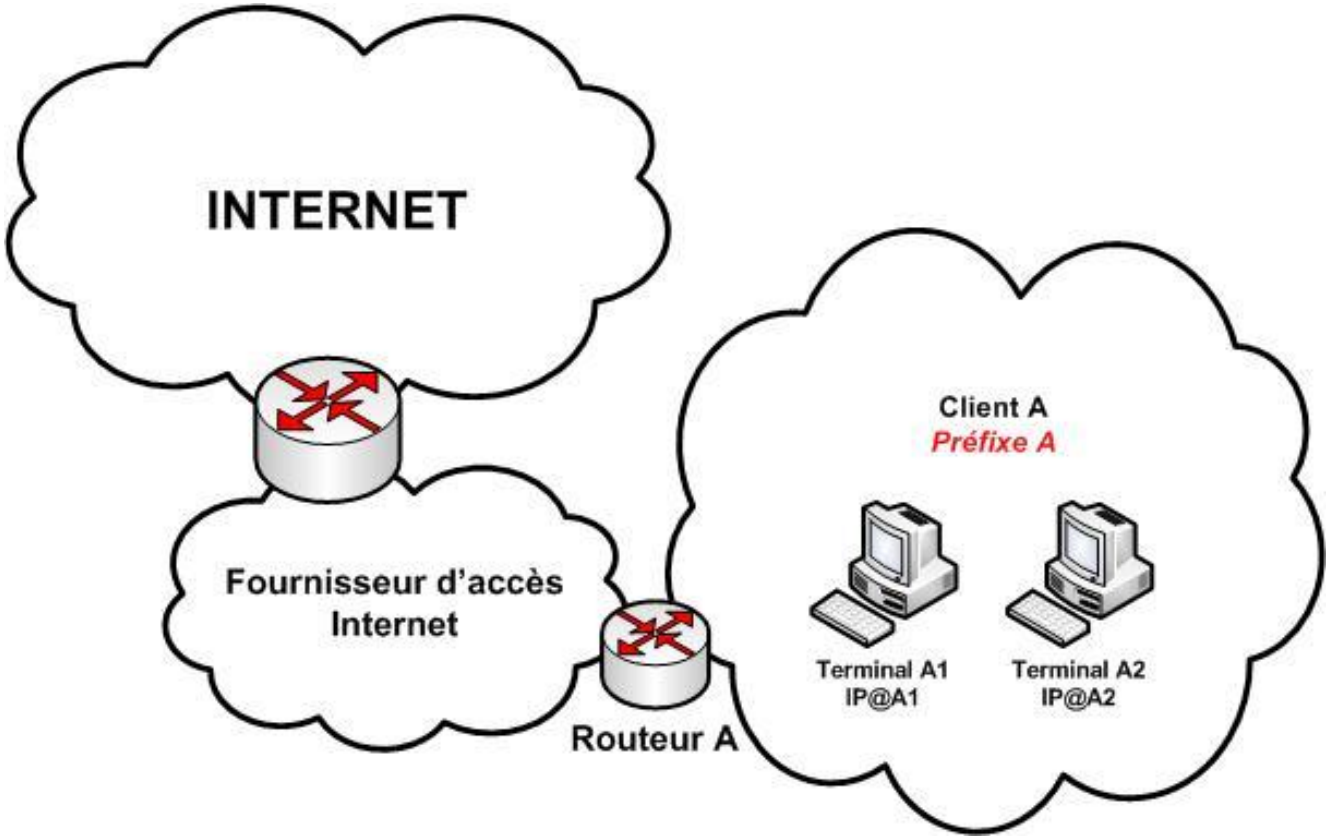
Limites

- Réseau "multihomé"



Limites

- Granularité



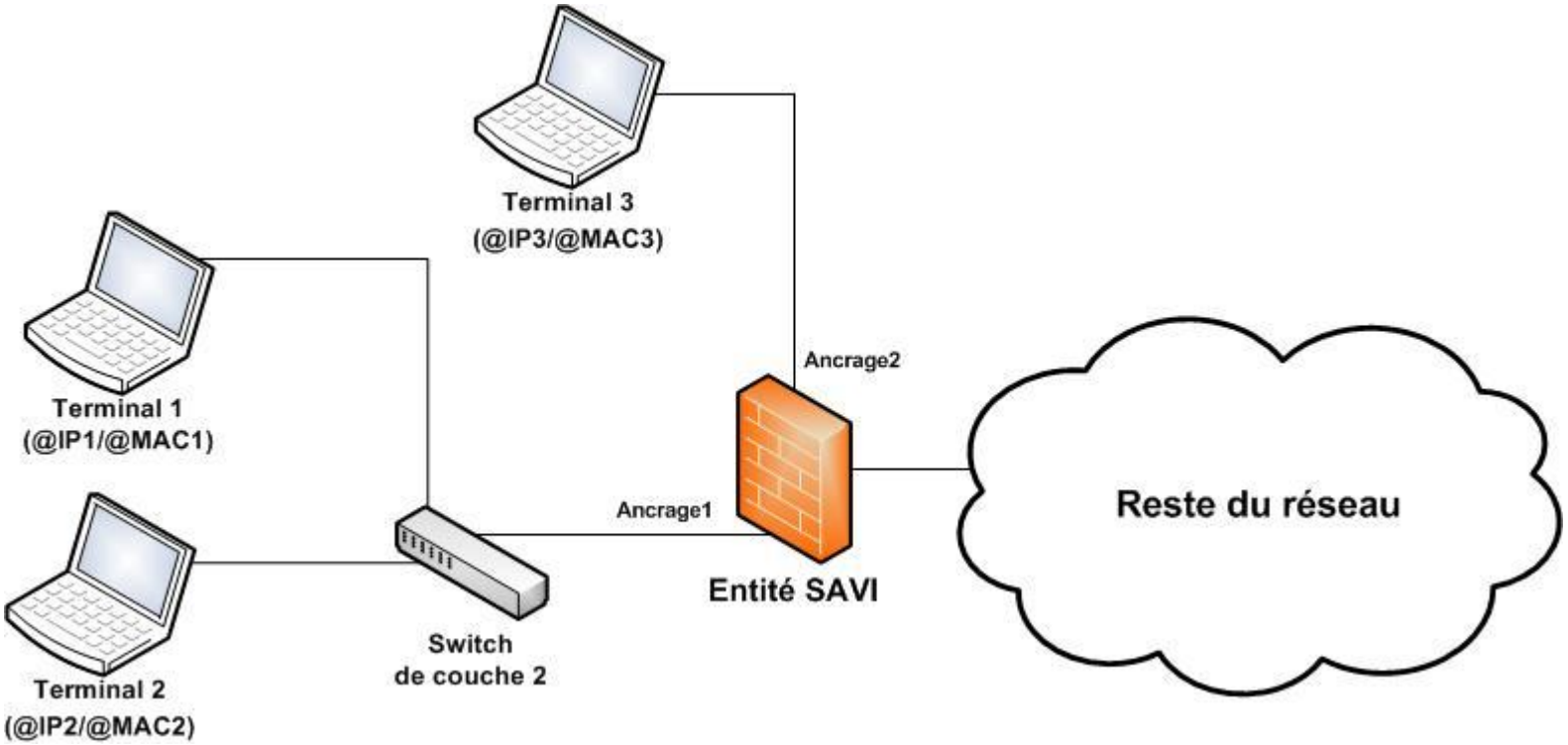
SAVI Principes

- IETF WG
- Juillet 2008
- Objectif : résoudre la dernière limite

Principes de SAVI

- draft-ietf-savi-framework
- Entité SAVI
  - Observe le trafic des terminaux IP
  - Observe la signalisation des protocoles d'assignation d'adresses IP (DHCPv4, DHCPv6, SLAAC, SEND)
  - Déterminer qui est le propriétaire légitime d'une adresse IP
  - En coupure des flux (e.g., switch L2, routeur, AP)
- Binding Anchor
  - Identifiant "ce" qui relie un terminal IP au réseau
    - port de switch
    - interface réseau, adresse MAC
    - 802.1X SA

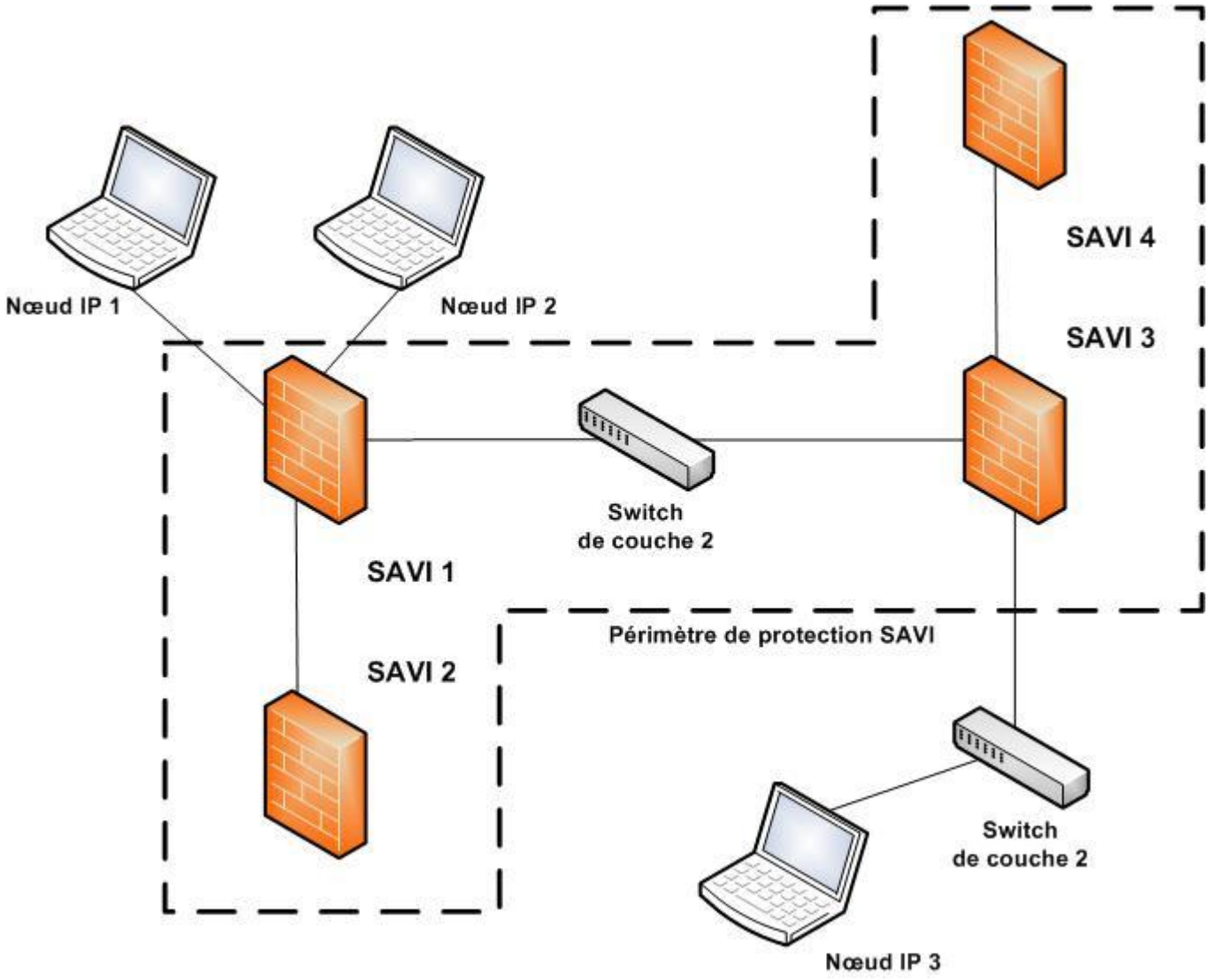
Principes de SAVI



Principes de SAVI

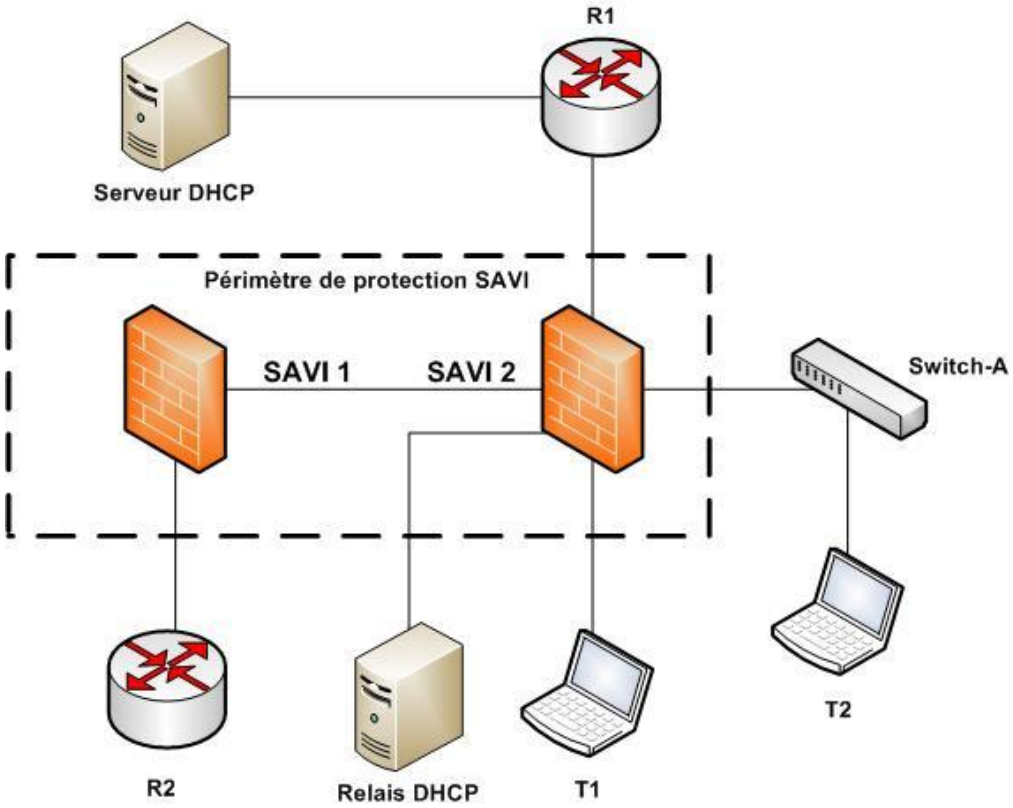
- SAVI Binding
  - Couple <Adresse IP, Binding Anchor>
- Règles de filtrage
  - Default: DENY ALL
  - Paquet IP légitime (i.e., ALLOW)
    - Pour un paquet IP d'adresse **`@IP`**
    - Arrivant via le Binding Anchor **`BA`**
    - Il existe un SAVI Binding <**`@IP`**,**`BA`**>
- Mécanisme de restauration des SAVI Bindings
- Périmètre de protection SAVI
  - Optimisation des ressources des entités SAVI
  - Validating Port (VP), Trusted Port (TP)

Principes de SAVI



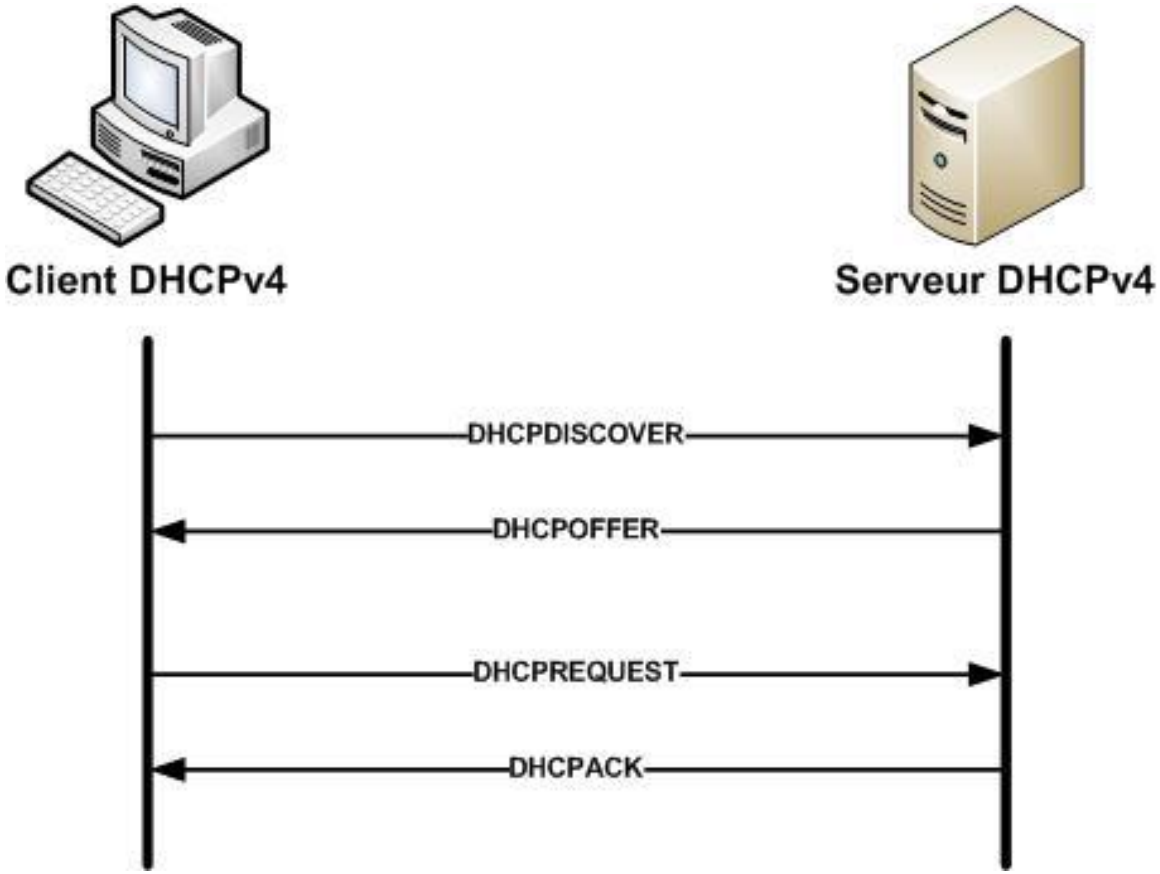
DHCP SAVI

- draft-ietf-savi-dhcp



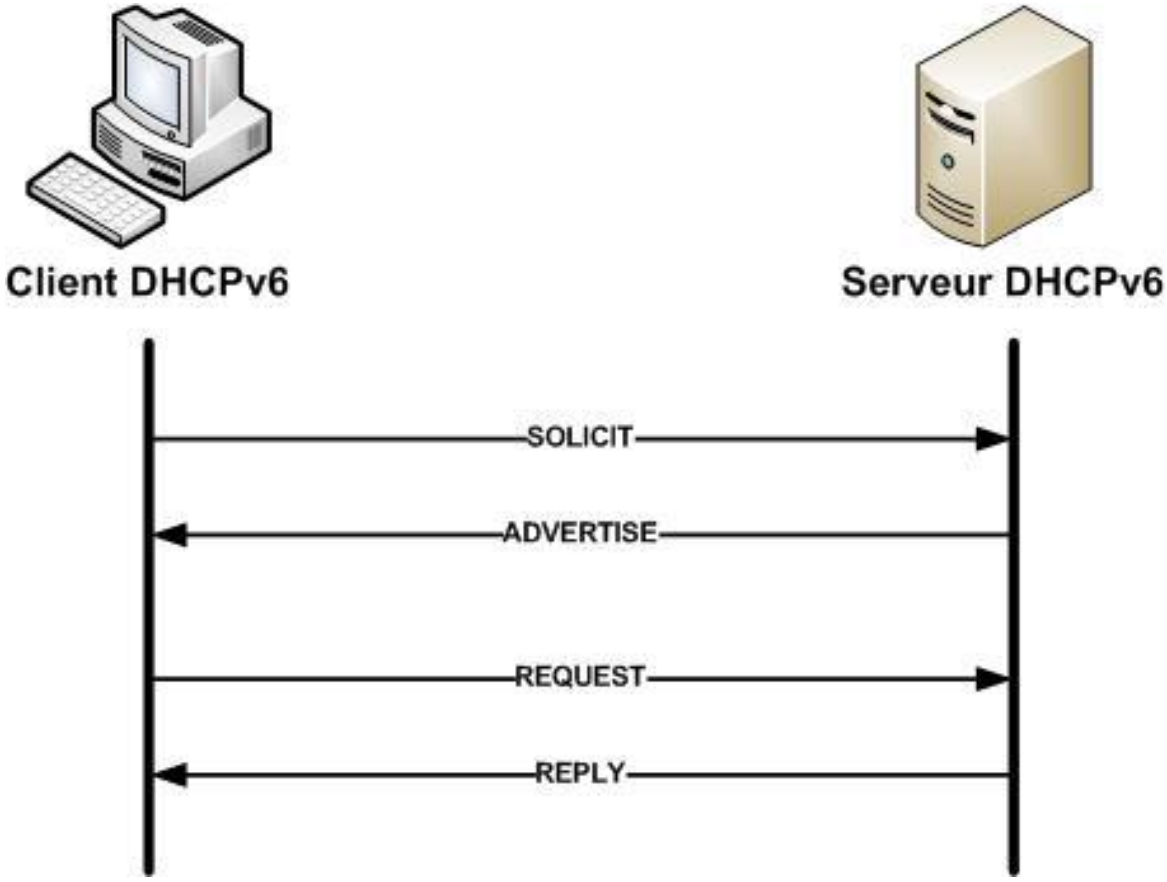
DHCP SAVI

- DHCPv4



DHCP SAVI

- DHCPv6

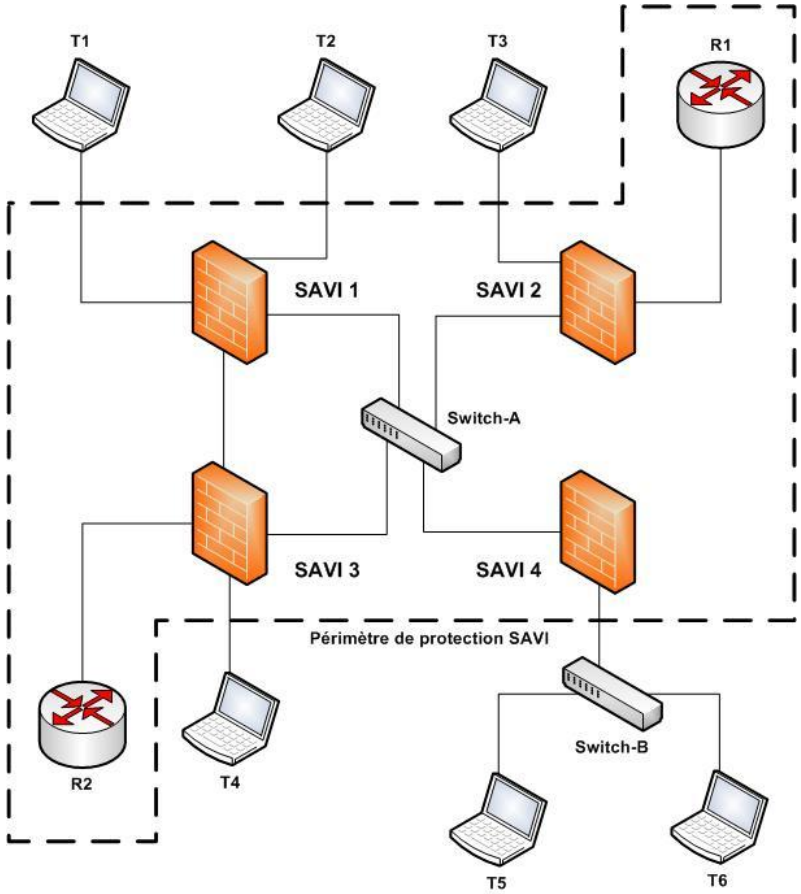


DHCP SAVI

- Base de données
  - Binding State Table (BST)
  - Filtering Table (FT)
- Mécanisme de restauration de SAVI Binding
  - Unicité de l'adresse : ARP/Duplicate Address Detection (DAD)
  - Adresse allouée par un serveur DHCP (DHCP LEASEQUERY)

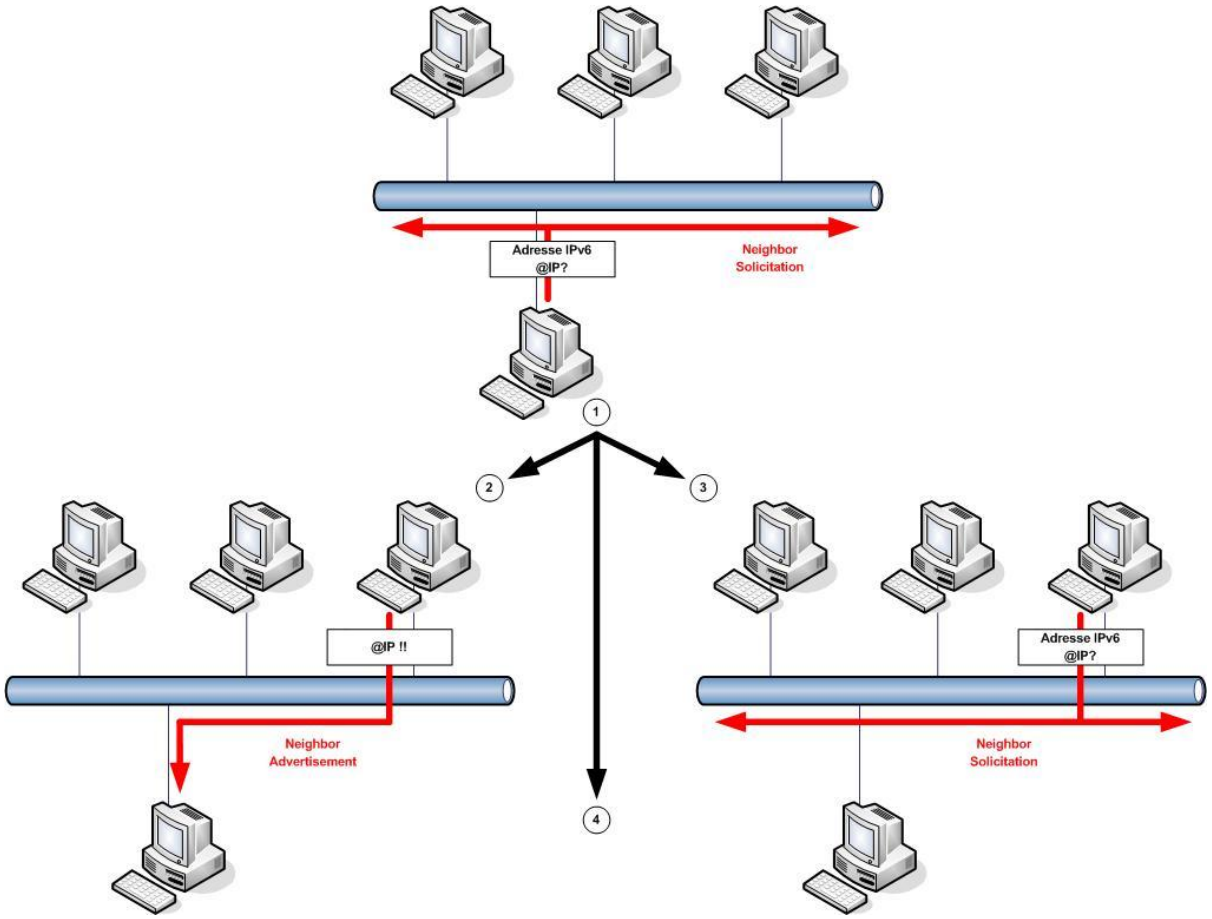
FCFS SAVI

- "First Come First Serve" (FCFS), pour SLAAC
- RFC 6620



FCFS SAVI

- SLAAC/DAD

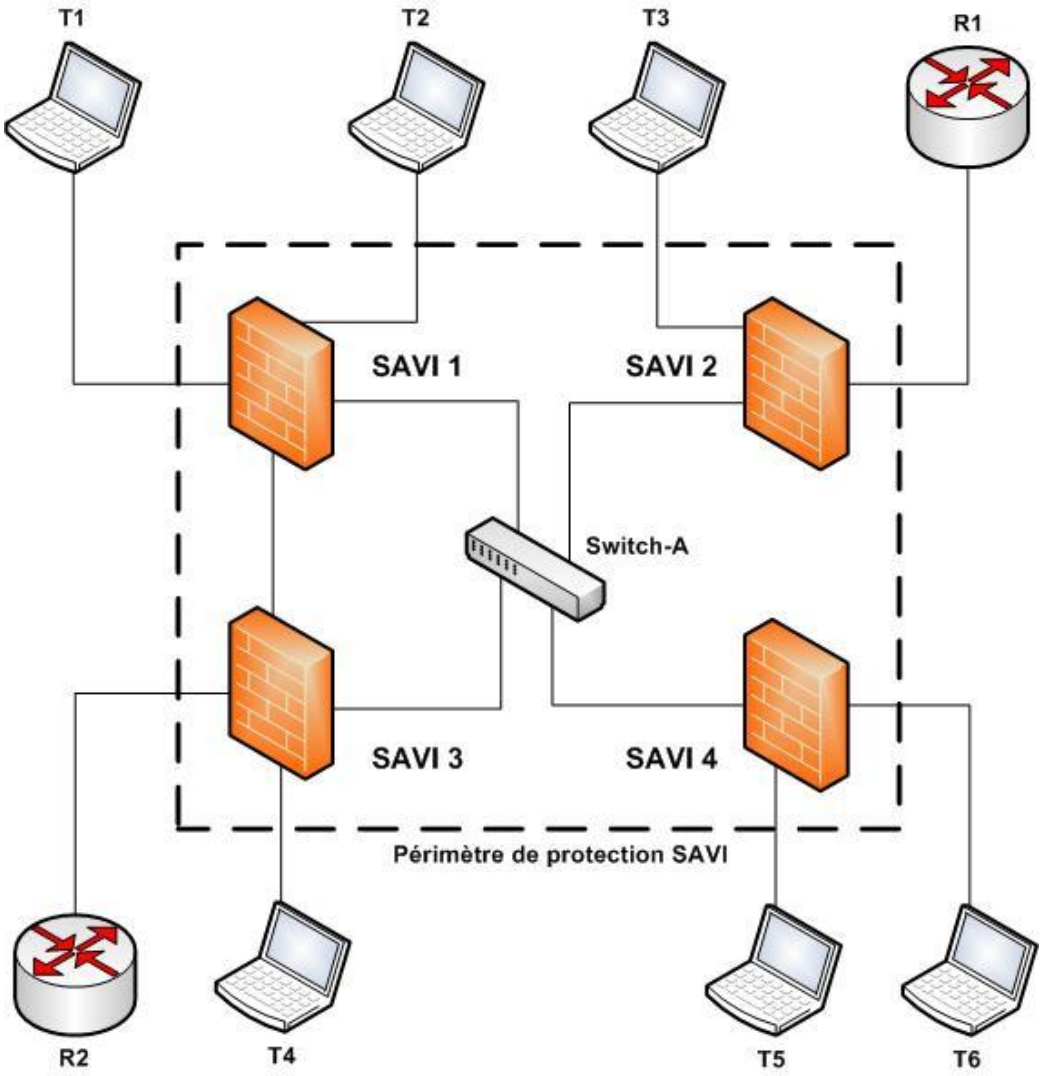


FCFS SAVI

- Base de données
  - FCFS SAVI Database (FCFS SAVI DB)
  - FCFS SAVI Prefix List (FCFS SAVI PL)
- Mécanisme de restauration de SAVI Binding
  - DAD (L'Entité SAVI usurpe l'adresse IPv6 du nœud ☺)

SEND SAVI

- draft-ietf-savi-send



SEND SAVI

- Secure Neighbor Discovery (SEND)
  - Utilisation de CGA
    - adresse IPv6 générée cryptographiquement
    - preuve de la possession d'une adresse IPv6
  - Utilisation de certificat X.509
    - preuve de l'autorisation d'être un routeur
  - Signature de la signalisation Neighbor Discovery
    - SLAAC/DAD

FCFS SAVI

- Base de données
  - SEND SAVI Database (SEND SAVI DB)
  - SEND SAVI Prefix List (SEND SAVI PL)
  - SEND SAVI Router List (SEND SAVI RL)
- Mécanisme de restauration de SAVI Binding
  - Neighbor Unreachability Detection (NUD)

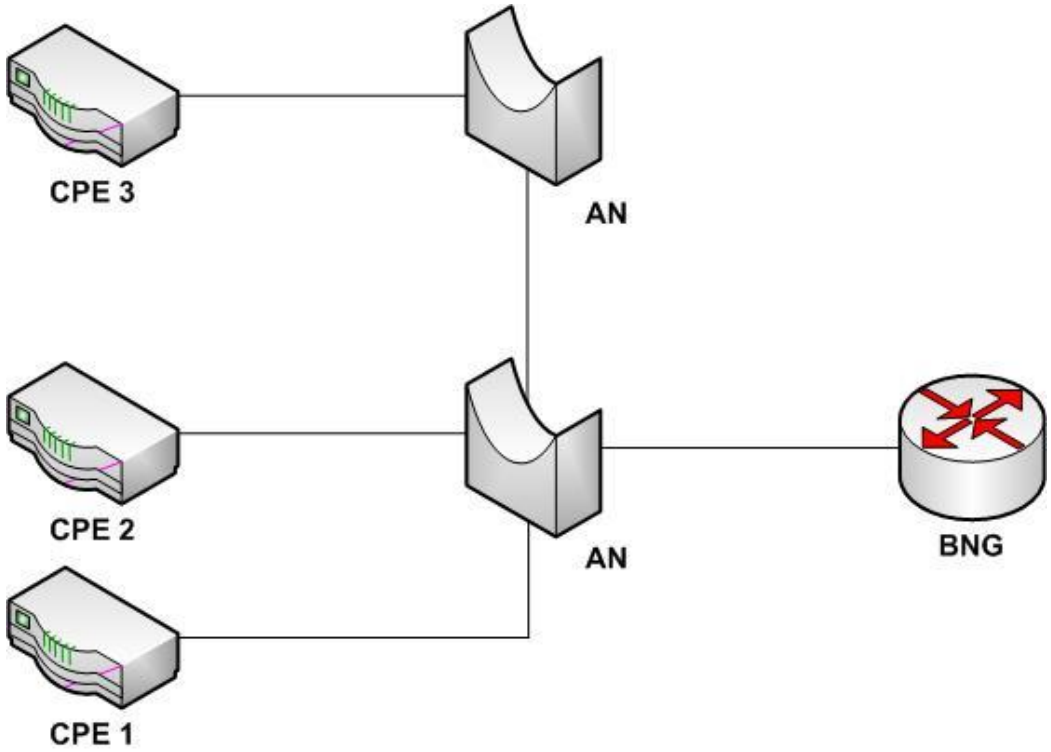
    => L'entité SAVI doit être un nœud IPv6 configuré

MIX SAVI

- draft-ietf-savi-mix
- Plusieurs solutions SAVI déployées
- Risque de collisions de SAVI Binding
- Recommendations pour limiter ce risque

Intégration/Implémentation/Déploiement

- Exemple d'intégration de SAVI
- Architecture IPv6 ADSL/Fibre de type "split-horizon forwarding, standardisée au BBF



Intégration/Implémentation/Déploiement

- FCFS SAVI (ou SEND SAVI)
- Entité SAVI
  - BNG
- Binding Anchor
  - Adresse MAC du CPE
  - Unicité garantie grâce à VMAC (fournie par l'AN)

Intégration/Implémentation/Déploiement

- Solutions officiellement implémentées
  - draft-ietf-savi-dhcp, version 7
  - draft-bi-savi-stateless, version 1
  - draft-bi-savi-mix, version 4 (partiellement)
  - draft-an-savi-mib, version 0
- Constructeurs
  - ZTE, Huawei, H3C
  - Ruijie, Digital China
  - Bitway, Centac

Intégration/Implémentation/Déploiement

- CERNET 2, switch L2, 1 Million de personnes impactées

Limites de SAVI

- Fragmentation
  - Entité SAVI capable de ré-assembler les fragments ?
- Optimistic DAD (oDAD)
  - Utilisation d'une adresse IPv6 avant la fin du processus DAD
  - Rejet des paquets si SAVI
- "Privacy"
  - Moyen de localiser de manière fiable une adresse IP
  - Utile au niveau administration d'un réseau
  - Problème de vie privée (e.g., utilisation adresses IPv6 aléatoires)

  => décision de l'IESG :

  log des tentatives d'usurpation SEULEMENT

Potentiels futurs travaux à l'IETF

- Court terme
  - MIB (pour SNMP)
- Moyen terme
  - Révision des spécifications
- Long terme
  - Solutions SAVI pour d'autres protocoles (e.g., IKEv2)

merci

orange™