

# **SUBADDRESS AND PORT SCRAMBLING (SAPS)**

## **A approach to avoid NAT drawbacks in IPv6**

IETF 73 - Minneapolis – 2008/11/21- Behave WG – Rémi Després

# Problem statement (1)

## NAT44 drawbacks

- **One point of failure**
- **Incoming connections made difficult**
  - ➔ **Port forwarding, STUN, TURN, UpNP, NAT-PMP etc.)**
- **E2E transparency is missing for:**
  - **Protocol independent call-backs and referrals**
  - **Host controlled multi-homing (e.g. for SCTP)**

# **Problem statement (2)**

## **NAT44 functions that can be useful in IPv6**

- 1. Local addressing independence (Easy renumbering)**
- 2. multi-homed CPEs**
- 3. Incoming connection filtering**
- 4. TOPOLOGY HIDING (invisibility of private routing plans)**
- 5. HOST PRIVACY (no visible association of connections to individual hosts)**

# Are NATs needed in IPv6?

- **Local addressing independence: Margaret's proposed 1:1 mapping**
- **Multihoming: SAMs - ref. draft-despres-sam**
- **Incoming connection filtering: above IP (same in IPv4 and IPv6)**
- **TOPOLOGY HIDING AND HOST PRIVACY statelessly ? See next**

# Subaddress And Port Scrambling (SAPS)

- **Scramble, at the customer edge, what you want to hide (multiply by a hidden key and place back in the same fields)**
- **If a local dynamic port is available (outgoing UDP, TCP etc.), then scramble subaddress, except IID type bit(s) and bits 2 to 15 of the port.**
- **Otherwise, just scramble the subaddress**
- **In incoming packets, unscramble**

# To be looked at

- **How to scramble only for hosts that want privacy, letting others being identifiable**
- **In multihomed sites, how to distribute safely to the CPEs the same key (if needed)**
- **See whether the scrambling key can be changed without breaking all existing connections**

# To conclude: A QUESTION

## What is best ?

- o Saying **IETF ENDORSES NAT66** (knowing that it will be taken as stateful as in NAT44)
- o Saying that **IETF DOES NOT ENDORSES NAT66**, but **ENDORSES NAC66** (or some other name), which is stateless

**IMHO, needs further thought**