Lightweight 4over6
+
SD-nat (aka stateless DS-Lite)
=
Lightweight DS-Lite
(twice as light!)

Peng Wu

Ian Farrer

Introduction

History

- ## Lightweight 4over6-05
  - Merge two documents
    - I-D.cui-softwire-b4-translated-ds-lite
    - I-D.zhou-softwire-b4-nat
  - Focus on architectural discussion
    - Current I-D does not recommend any provisioning method. Rather it suggests it is up to operators to decide what to use.

- ## SD-Nat-02
  - Use minPort-maxPort ICMP message
    - instead of [1024-Maxport] only
    - No need for ALGs on AFTR
  - Focus on DS-Lite only
    - (no description of NAT444 case)

Motivations

- Extension to DS-lite with no NAT, and address sharing mode for Public 4over6
  - backward compatible

- IPv4 address sharing
  - Subscriber-level port set allocation

- Scalability requirement
  - Per-session=>per-subscriber state
  - Easy/No logging
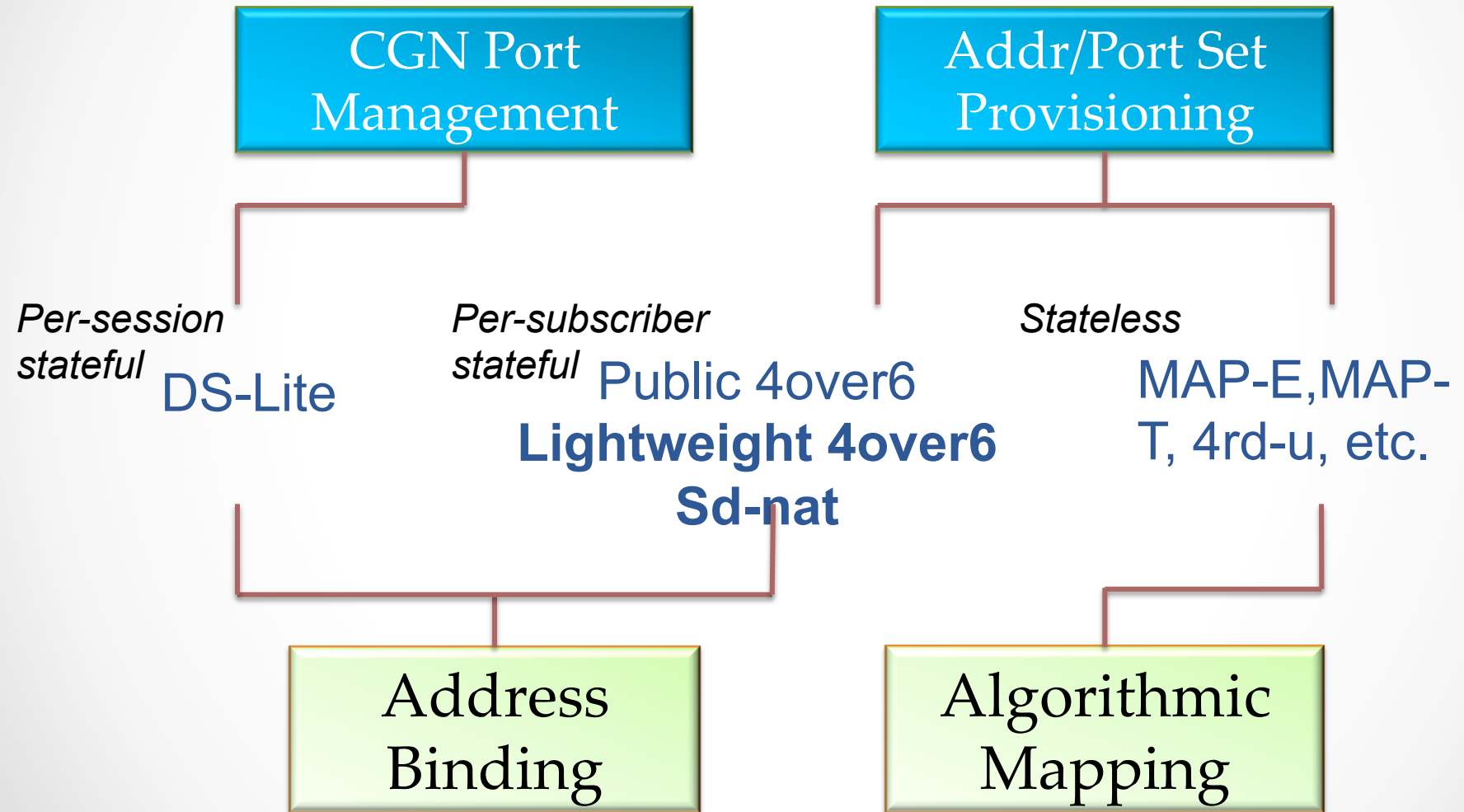
- No IPv4 and IPv6 address coupling

Benefits of allocating independently IPv6 and IPv4 address

- IPv6 addresses do not have to be allocated sequentially.

- Easily define and change IPv4 customer profiles (number of ports).

- IPv4 resources can be re-allocated freely.

- Anycast announcements can be fine tuned.

Not Tying IPv6 address to IPv4 address plus port range

- In general, removing the mathematical restriction allows the operator to deliver the service he wants to offer, in the way he wants to offer them.

- The price to pay is to provision and manage resources at a finer granularity.

- Introduce per-subscriber state on tunnel concentrator (AFTR)
  - No per flow state!

Technical Matrix

CGN Port Management

Addr/Port Set Provisioning

Per-session stateful
DS-Lite

Per-subscriber stateful
Public 4over6
Lightweight 4over6
Sd-nat

Stateless
MAP-E,MAP-T, 4rd-u, etc.

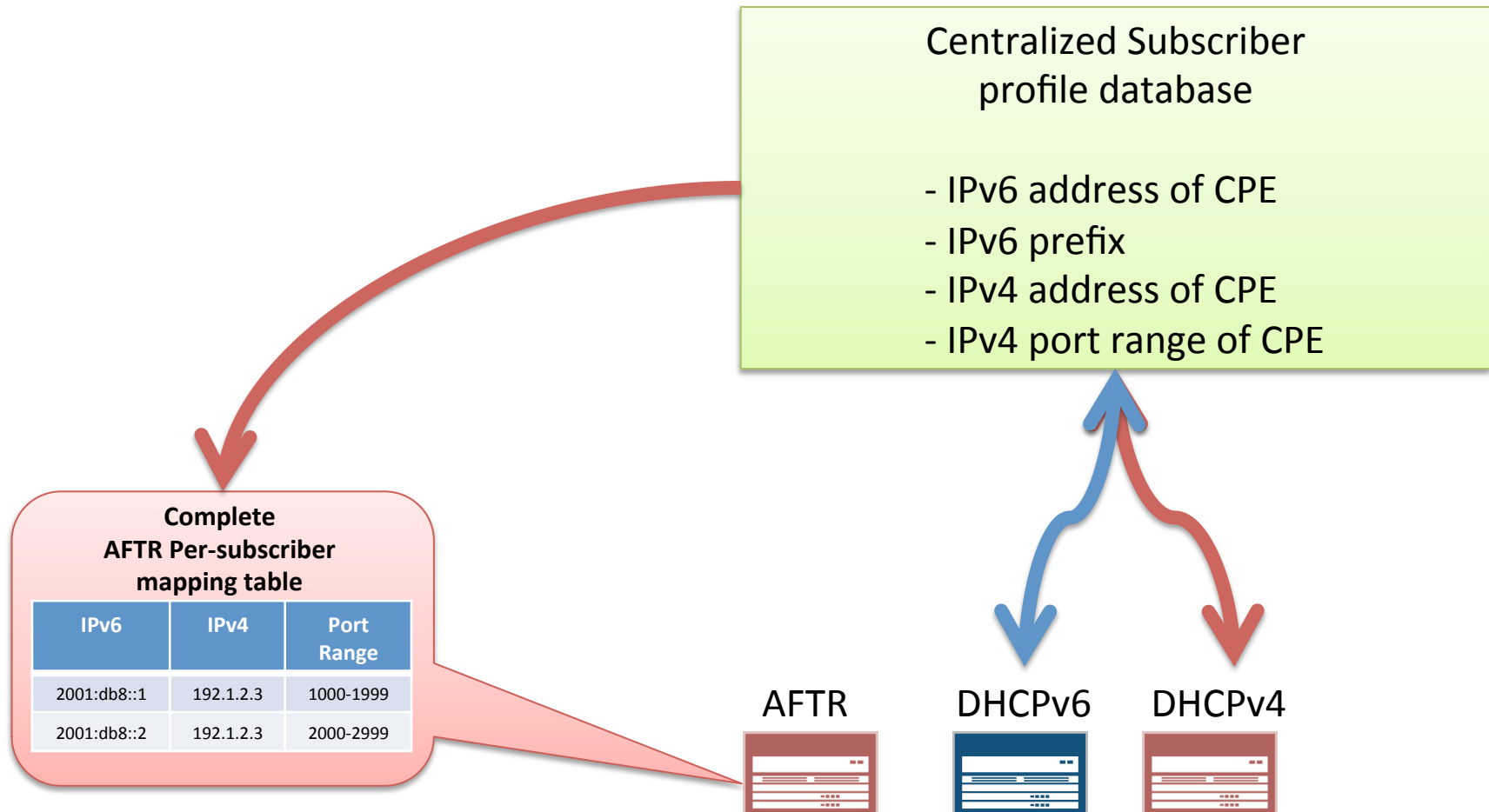Address Binding

Algorithmic Mapping

AFTR Provisioning Architecture

Role of AFTR

- Upstream
  - Decapsulate IPv6 header
  - Ingress filtering
    - ACL check on IPV4 address + port against per-subscriber mapping table
    - Send ICMP message back to CPE if ACL fails
- Downstream
  - Subscriber lookup
    - Check IPv4 address + port against per-subscriber mapping table
  - Encapsulate in IPv6

Top-Down subscriber management

Centralized Subscriber profile database

- IPv6 address of CPE
- IPv6 prefix
- IPv4 address of CPE
- IPv4 port range of CPE

**Complete
AFTR Per-subscriber
mapping table**

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

AFTR

DHCPv6

DHCPv4

Stateless Fail-over Architecture

Top-Down subscriber management

IPv4

Complete AFTR Per-user mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

P

P

IPv4 **anycast** route for **IPv4 NAT poo**l
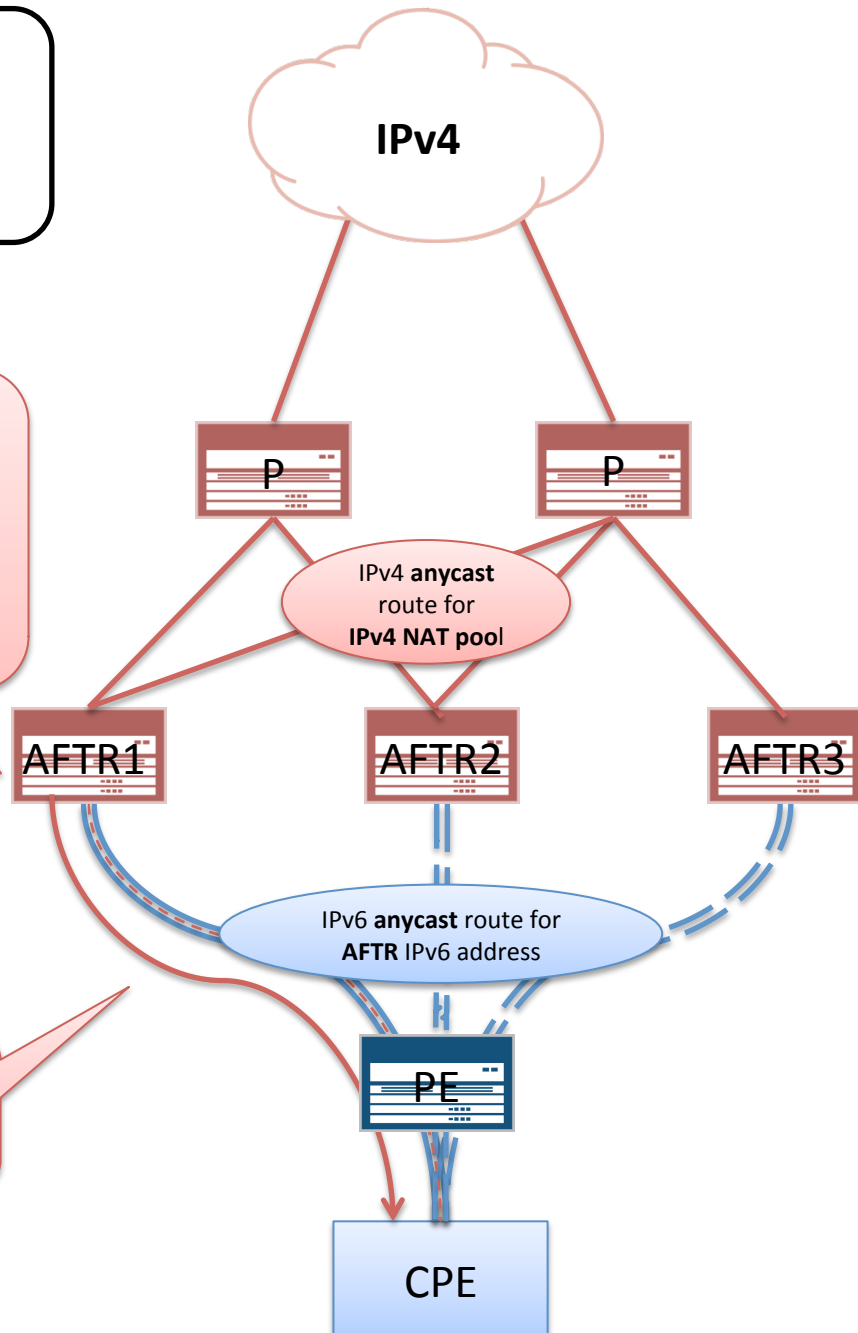
AFTR1

AFTR2

AFTR3

AFTR1, AFTR2 & AFTR3 are configured with the **same**:
- **IPv4 pool**
- **Per-user mapping table**
- **IPv6 AFTR address**

IPv6 **anycast** route for **AFTR** IPv6 address

ICMPv4 "Port Restricted" over IPv6 tunnel

PE

CPE

Bottom-Up subscriber management

Log database

- IPv6 address of CPE
- IPv6 prefix
- IPv4 address of CPE
- IPv4 port range of CPE

local AFTR Per-subscriber mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

DHCPv4
Server/Relay

Tunnel
Concentrator

AFTR box

No central database
to pre-allocate IPv4 or IPv6
customer information

DHCPv6

Local database:
No stateless fail-over
between AFTRs
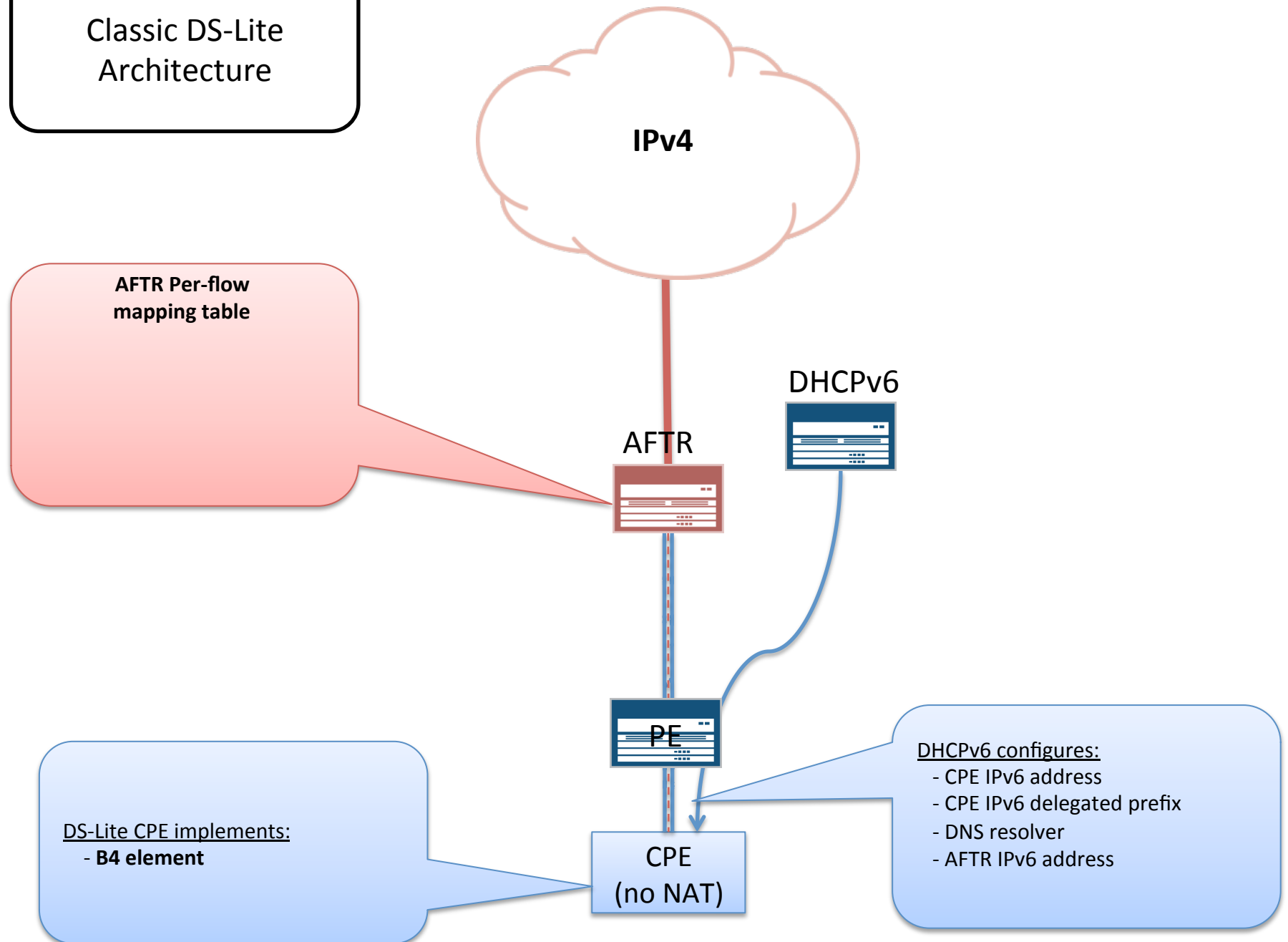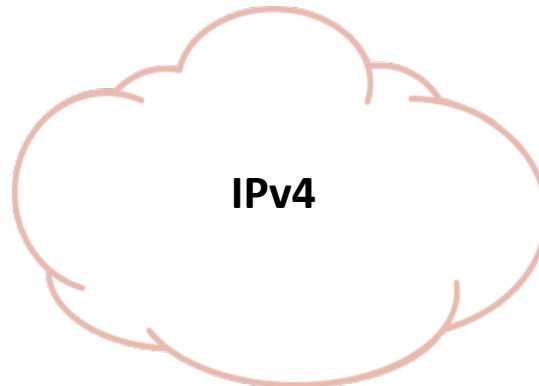
Trade-off
Top-Down vs Bottom-Up

- Bottom-Up
  - IPv4 addresses & ports managed locally by AFTRs
  - No centralized subscriber database of IPv4/IPv6 resources
  - Need per-subscriber logging to reconcile information
  - Fail-over similar to standard DS-Lite

- Top-Down
  - IPv4 addresses and port centrally managed
  - Each AFTR has same subscriber mapping table
  - Enable stateless fail-over between AFTRs

CPE Configuration Architecture

Classic DS-Lite
Architecture

IPv4

AFTR Per-flow
mapping table

DHCPv6

AFTR

PE

DHCPv6 configures:
- CPE IPv6 address
- CPE IPv6 delegated prefix
- DNS resolver
- AFTR IPv6 address

DS-Lite CPE implements:
- **B4 element**

CPE
(no NAT)

Public 4over6
Architecture

IPv4

AFTR Per-subscriber mapping table

IPv6	IPv4
2001:db8::1	192.1.2.3
2001:db8::2	192.1.2.3

AFTR

DHCPv6

DHCPv4

PE

__DHCPv4 (over IPv6) configures__
CPE B4 IPv4 address

Stateless DS-Lite CPE implements:
- **DHCPv4 Client Relay Agent**
  (over IPv6) to configure
  B4 element IPv4 address

CPE
(NAT)
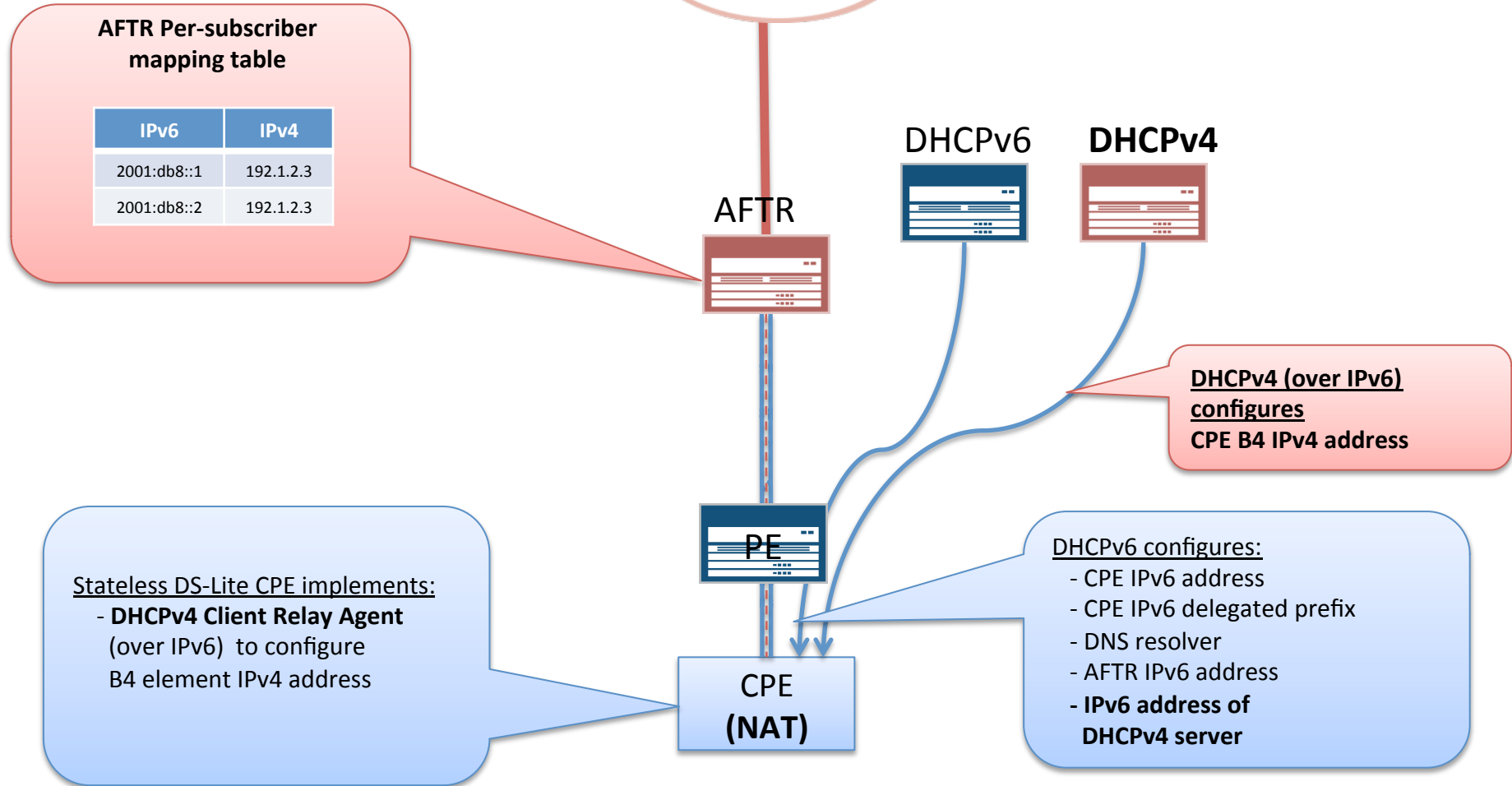
DHCPv6 configures:
 - CPE IPv6 address
 - CPE IPv6 delegated prefix
 - DNS resolver
 - AFTR IPv6 address
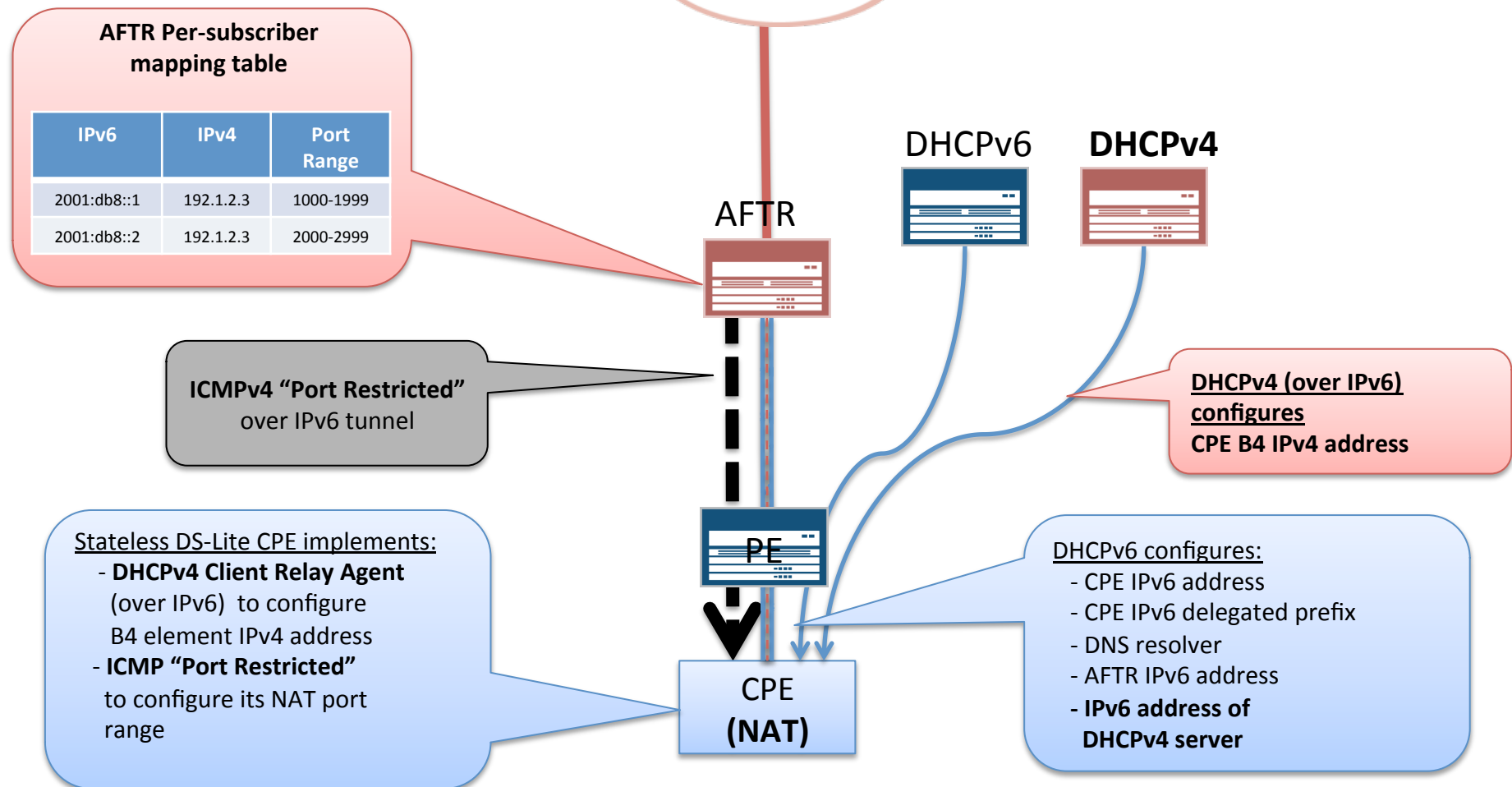 - **IPv6 address of**
   DHCPv4 server

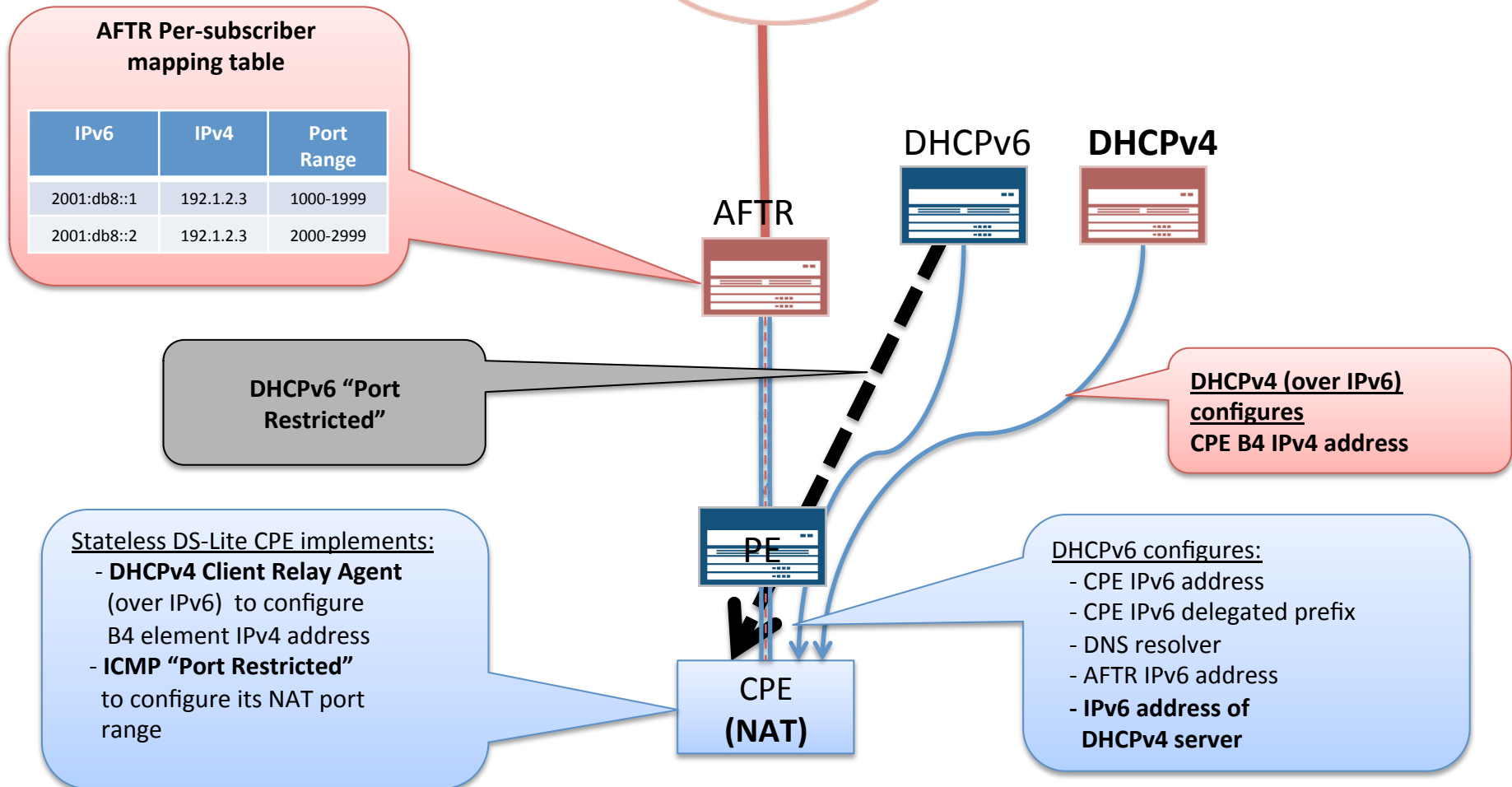# "lightweight DS-Lite" CPE Provisioning

- IPv4 address
  - DHCPv4 over IPv6
  - PCP

- IPv4 port range
  - ICMP
  - DHCPv4 over IPv6 option
  - DHCPv6 option
  - PCP option

→ We need to select one as mandatory to implement

Stateless DS-Lite Architecture

IPv4

AFTR Per-subscriber mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

AFTR

DHCPv6

DHCPv4

PE

ICMPv4 "Port Restricted" over IPv6 tunnel

DHCPv4 (over IPv6) configures CPE B4 IPv4 address

Stateless DS-Lite CPE implements:
- **DHCPv4 Client Relay Agent** (over IPv6) to configure B4 element IPv4 address
- **ICMP "Port Restricted"** to configure its NAT port range

CPE (NAT)

DHCPv6 configures:
- CPE IPv6 address
- CPE IPv6 delegated prefix
- DNS resolver
- AFTR IPv6 address
- **IPv6 address of DHCPv4 server**

Lightweight 4over6
Architecture
DHCPv6 variant

IPv4

AFTR Per-subscriber
mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

DHCPv6

DHCPv4

AFTR

DHCPv6 "Port Restricted"

DHCPv4 (over IPv6) configures
CPE B4 IPv4 address

PE

Stateless DS-Lite CPE implements:
 - **DHCPv4 Client Relay Agent**
   (over IPv6) to configure
   B4 element IPv4 address
 - **ICMP "Port Restricted"**
   to configure its NAT port range

DHCPv6 configures:
 - CPE IPv6 address
 - CPE IPv6 delegated prefix
 - DNS resolver
 - AFTR IPv6 address
 - **IPv6 address of DHCPv4 server**

CPE
(NAT)

Lightweight 4over6 Architecture DHCPv4 variant

IPv4

AFTR Per-subscriber mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

AFTR

DHCPv6

DHCPv4

DHCPv4 "Port Restricted"

DHCPv4 (over IPv6) configures CPE B4 IPv4 address

PE

Stateless DS-Lite CPE implements:
- **DHCPv4 Client Relay Agent** (over IPv6) to configure B4 element IPv4 address
- **ICMP "Port Restricted"** to configure its NAT port range

CPE (NAT)

DHCPv6 configures:
- CPE IPv6 address
- CPE IPv6 delegated prefix
- DNS resolver
- AFTR IPv6 address
- **IPv6 address of DHCPv4 server**

# Lightweight 4over6 Architecture PCP variant

IPv4

PCP

DHCPv6   **DHCPv4**

AFTR

PE

CPE
(NAT)

AFTR Per-subscriber mapping table

IPv6	IPv4	Port Range
2001:db8::1	192.1.2.3	1000-1999
2001:db8::2	192.1.2.3	2000-2999

PCP "Port Restricted" message

DHCPv4 (over IPv6) configures
CPE B4 IPv4 address

Stateless DS-Lite CPE implements:
- **DHCPv4 Client Relay Agent** (over IPv6) to configure B4 element IPv4 address
- **ICMP "Port Restricted"** to configure its NAT port range
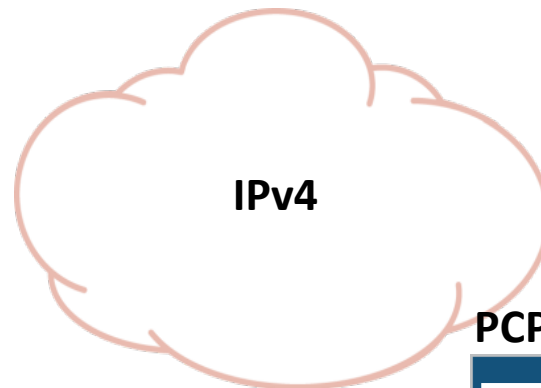
DHCPv6 configures:
- CPE IPv6 address
- CPE IPv6 delegated prefix
- DNS resolver
- AFTR IPv6 address
- **IPv6 address of DHCPv4 server**

Proposal: ICMP port restricted message as minimum mandatory to implement

- AFTR need to be provisioned with per-subscriber mapping information to enforce ingress filtering

- AFTR must notify the CPE when port is out of assigned range

- Need a new ICMP message type for that

- **Just use it to carry correct port range information!**

Adding other mechanisms as optional to implement

- DHCPv4 port range option
- PCP port range option

- If CPE is implementing an optional method, it must take intersection of ICMP information and optional method information.

Next Steps

Moving Forward

- Merge two proposals
- Create two new documents:
  - Document 1:
    - General framework (NAT in CPE, Binding table in AFTR)
    - Trade-off between Top-Down and Bottom-up AFTR provisioning model
    - Backward compatibility with DS-Lite & public 4over6
  - Document 2:
    - CPE protocols
      - Reference to DHCPv4 over IPv6 for IPv4 address
      - ICMP port-restricted as minimum mandatory to implement
      - Optional port allocation methods: DHCPv4 & PCP options