

Detecting CGN in the ISP

kc claffy, Amogh Dhamdhere, Andra Lutu, Marcelo Bagnulo

Presentation to MBA group

15 December 2015

Motivation: Perspectives on CGN

- CGN is perceived as an impediment to fully benefiting from IPv6 deployment
 - especially to carriers who invest in IPv6
- There is thus growing interest in measuring CGN deployment
 - Always a chance of false positives
- Better to have good data than bad data on this issue
- We want to validate a method that can be used by others to accurately determine CGN deployment

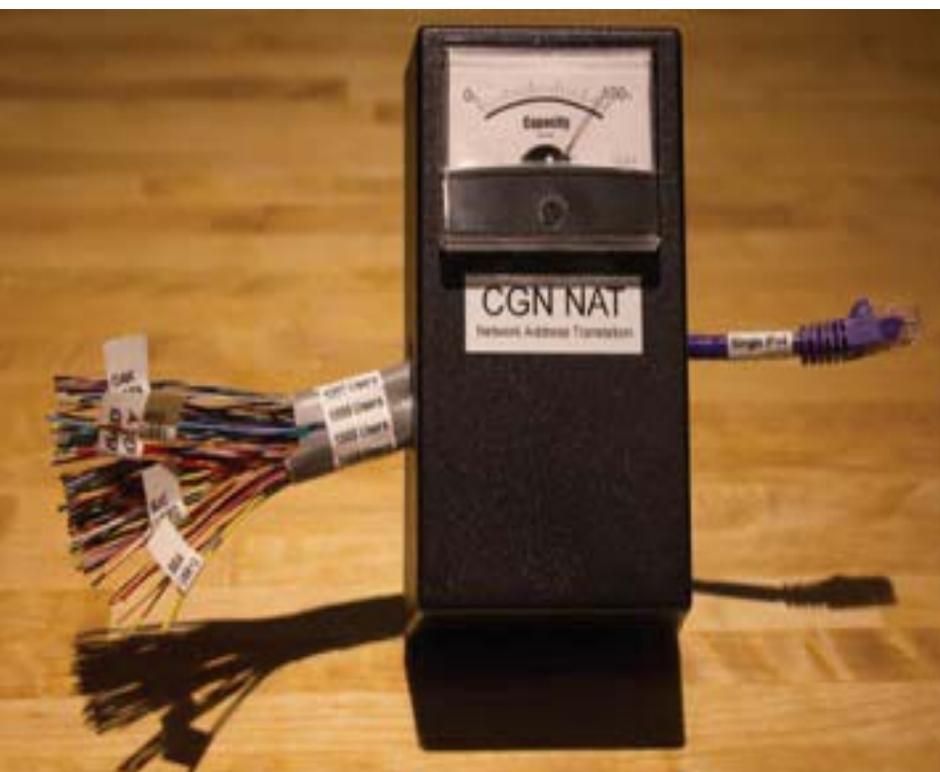


Network Address Translation (NAT)

- The success of the Internet led to the depletion of the IPv4 address space
- IPv6 - only viable solution, very slow adoption
- Network Address Translation – prolongs the life of IPv4, by enabling address sharing
- Tradeoffs:
 - As broadband becomes prevalent, NAT devices turn into performance bottlenecks
 - NAT hinders certain applications (e.g., VoIP)
 - Breaks Internet end-to-end principle
 - Inhibits the conversion to IPv6 in the medium term



NAT444 / Carrier Grade NAT/ Large Scale NAT



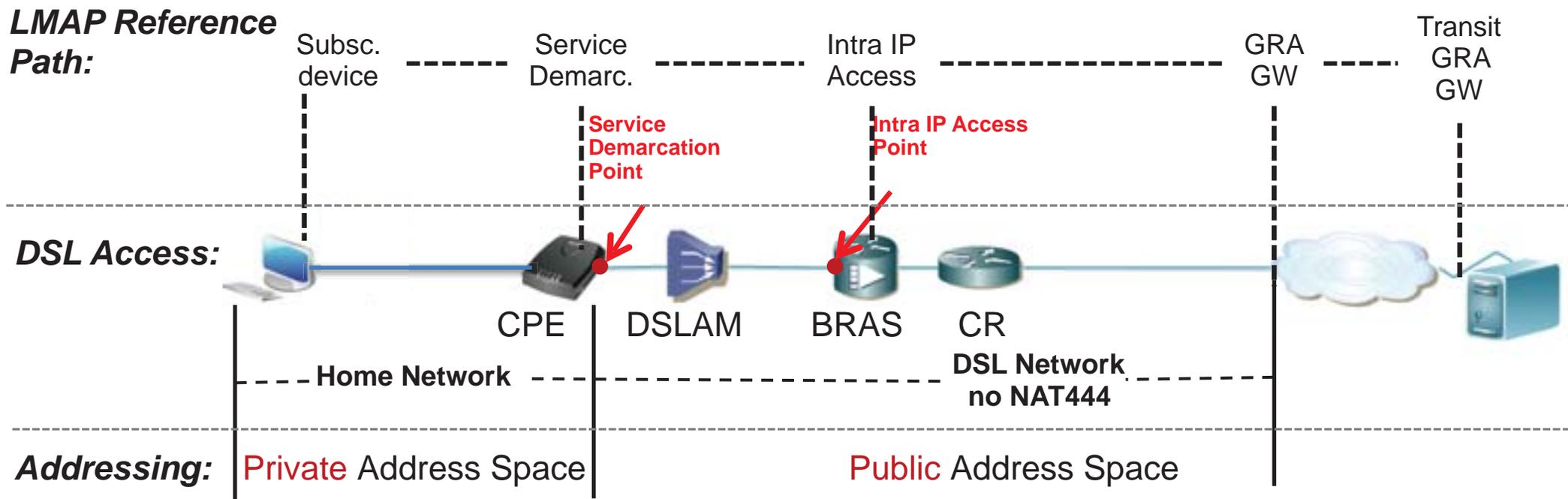
RFC7021: Assessing the Impact of Carrier-Grade NAT on Network Applications

- On-line gaming
- Video streaming
- BitTorrent
- VPN & Encryption
- VoIP
- ... etc.



Traditional NAT (NAT44)

DSL Access Network mapped to the LMAP Reference Path

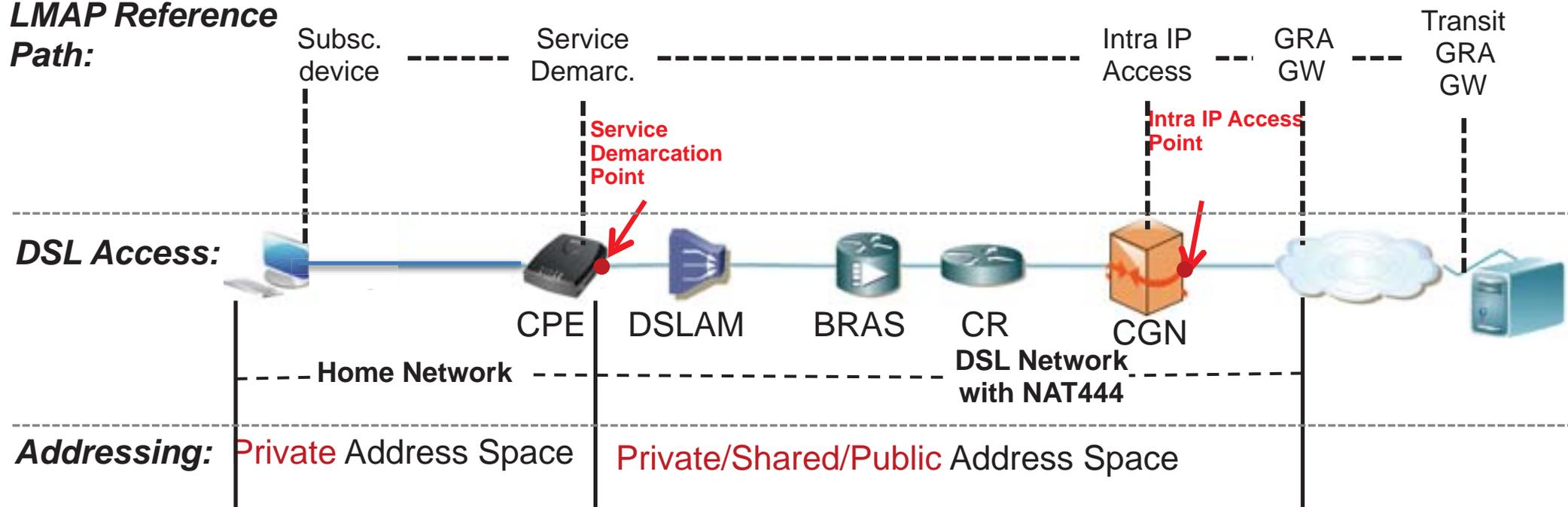




Large Scale NAT (NAT444)

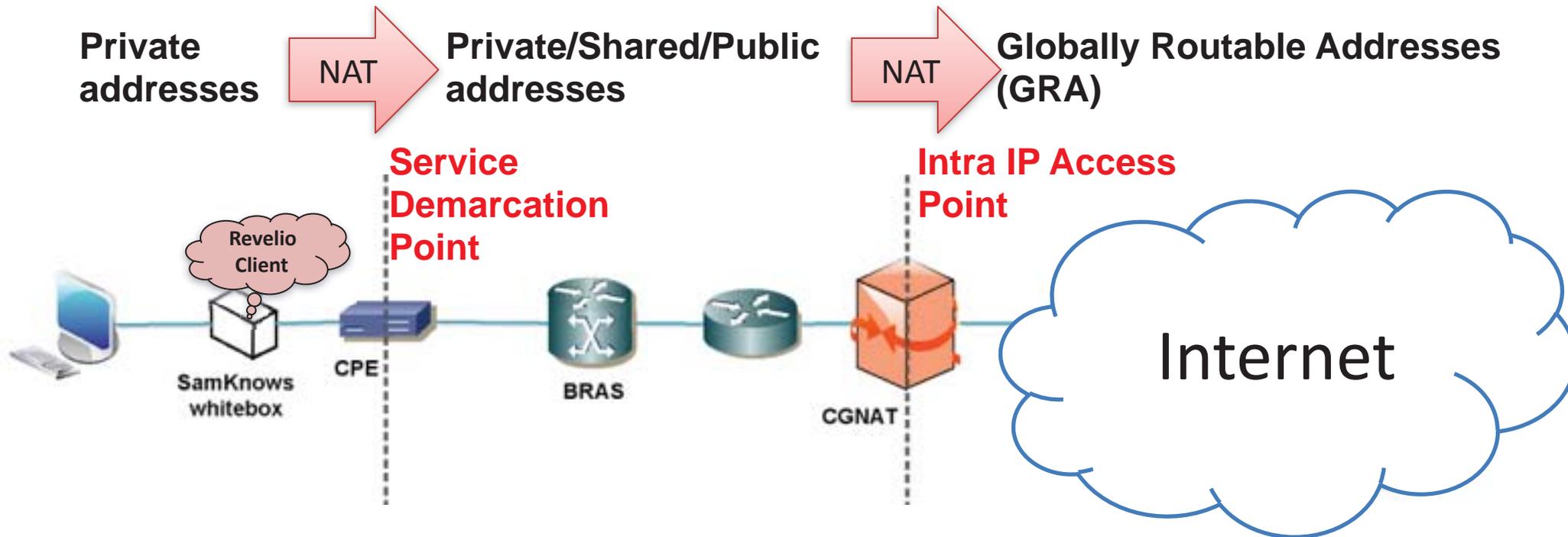
DSL Access Network *with NAT444 deployment*

LMAP Reference Path:



NAT Revelio

for Measuring Broadband America (MBA)

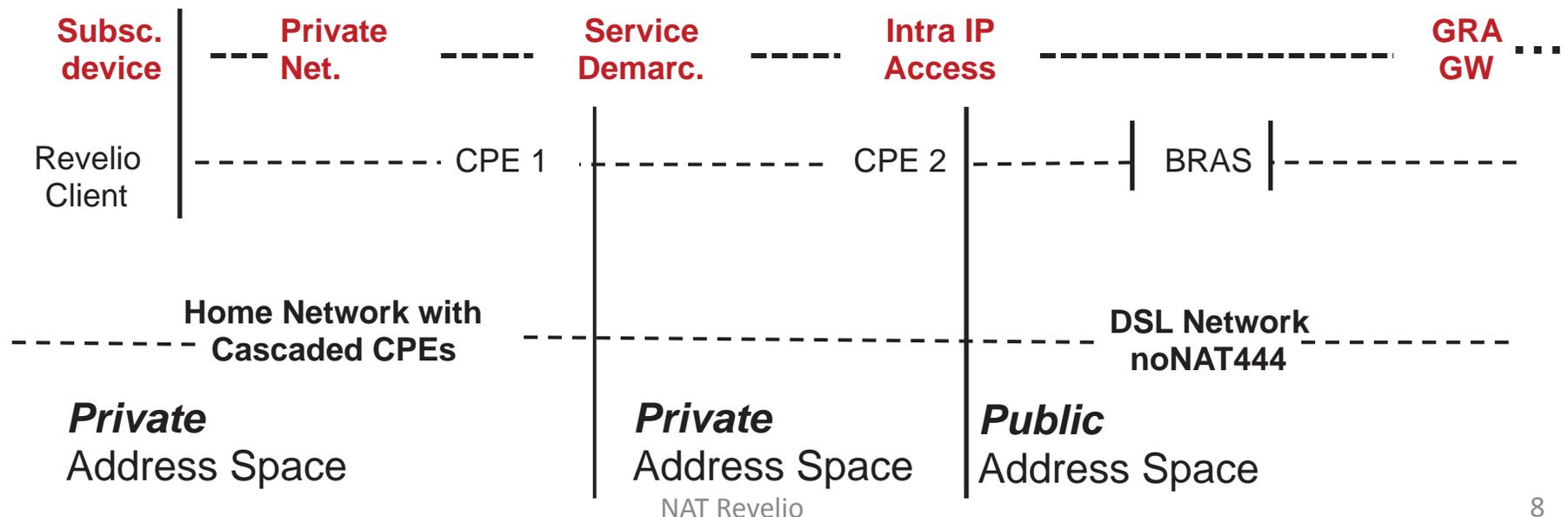


- Detect the usage of *private/shared address space* beyond the Service Demarcation device (CPE), in the ISP access network
- Detect the location (*home network or ISP access network*) device doing the translation to the GRA of the subscriber

NAT Revelio: Design Challenges

- Avoid NAT444 false positives:
 - Diverse home network configurations, e.g. In-home cascaded NAT, with probe **NOT** connected directly to the CPE (Service Demarcation device), misconfiguration in setting up FCC MBA box
 - Diverse ISP configurations and deployments, e.g. use of private IP addresses internally even if they don't do NAT444

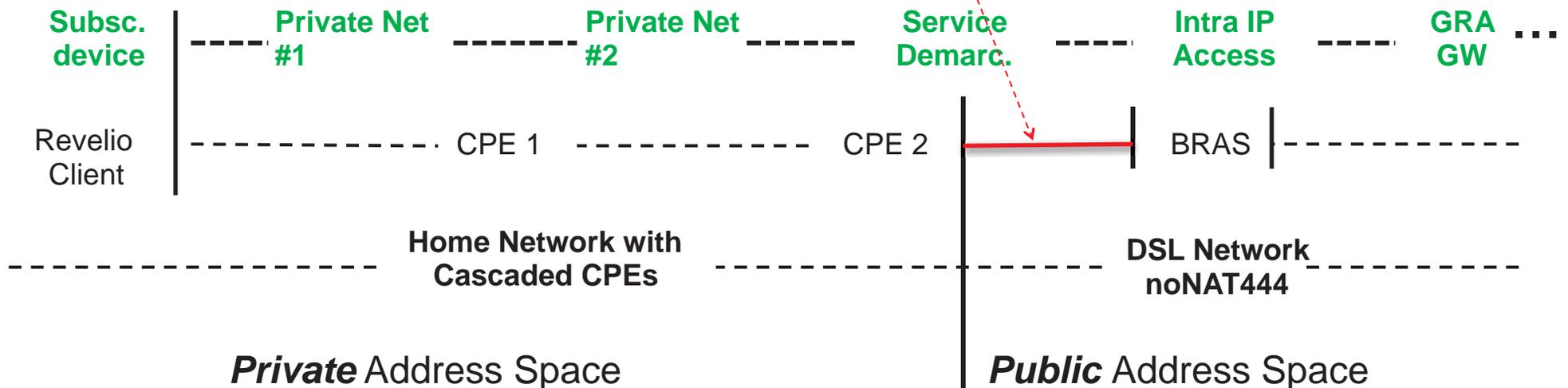
Incorrect Mapping with the LMAP Reference Path:



NAT Revelio: Design Challenges

- Need to detect the *access link*, to delimit the *access network* and the *home network*
- Allows to eliminate some false positives

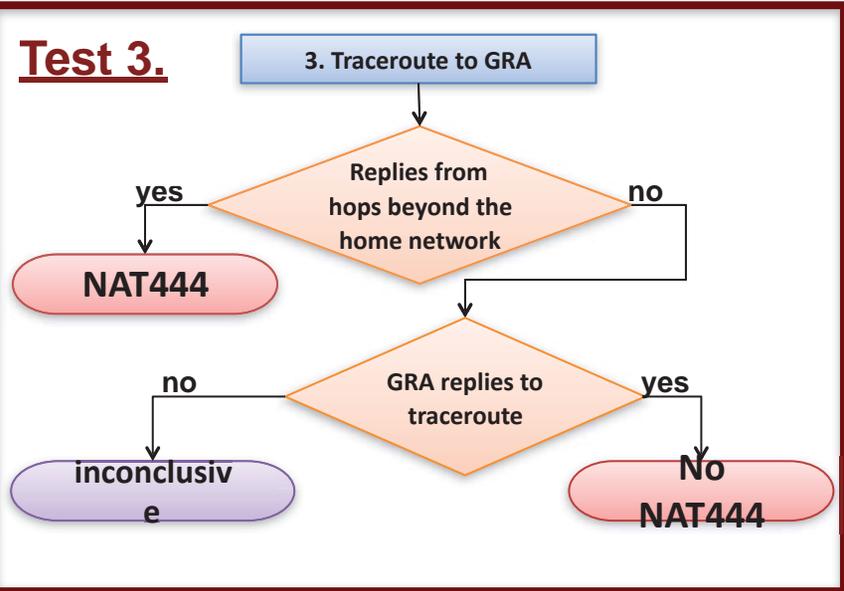
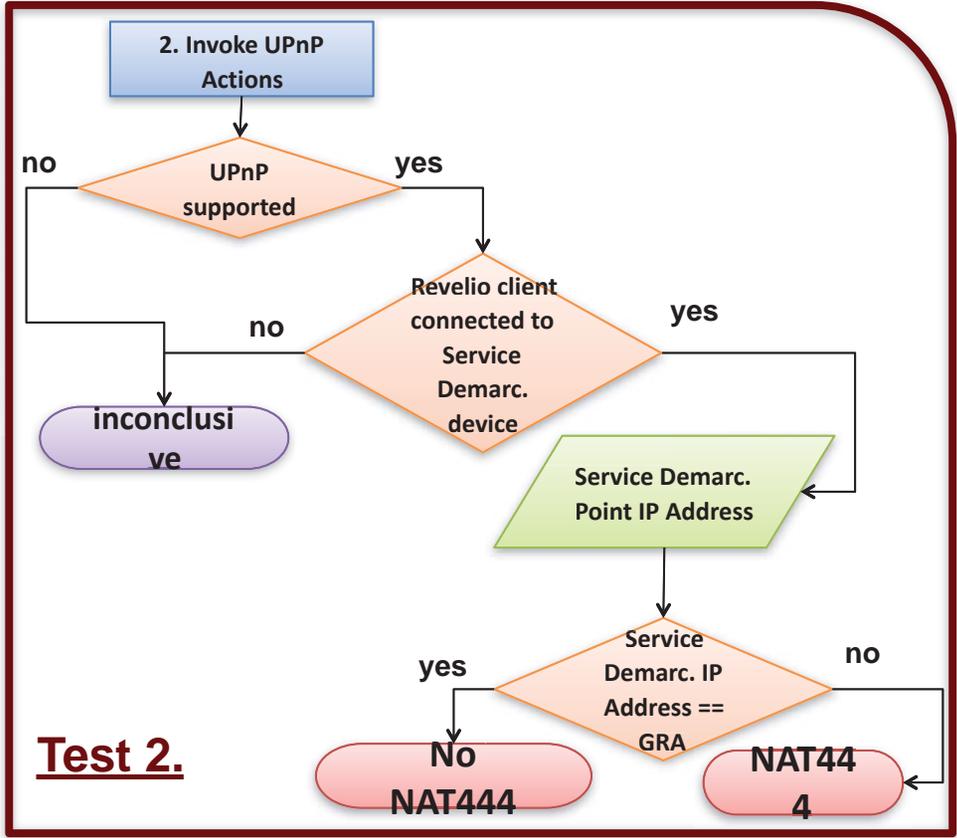
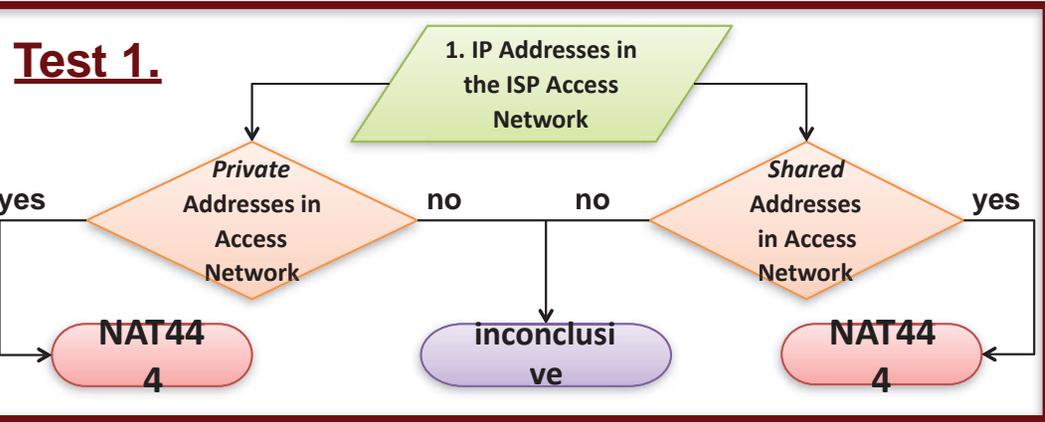
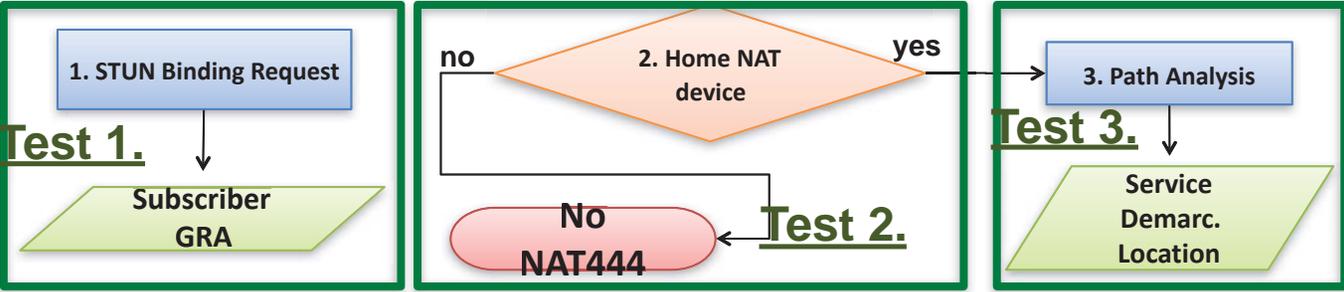
Correct Mapping with the LMAP Reference Path



NAT Revelio

- The NAT Revelio test suite includes 2 phases:
 - ***Environmental Characterization***
 - *Understand the environment hosting the device running the Revelio Client*
 - ***NAT444 Discovery***
 - *Detection of signals that the ISP might deploy a NAT444 solution in the ISP access network*

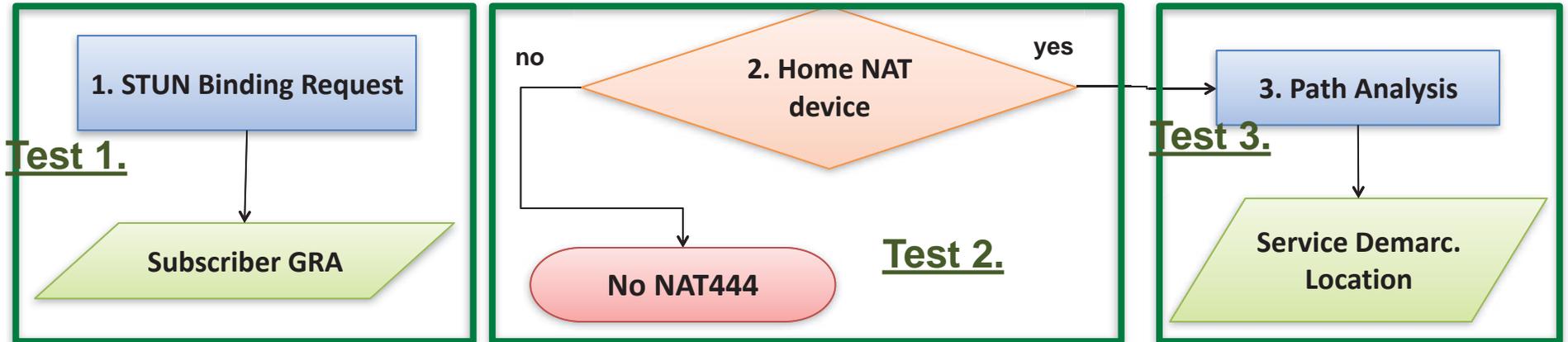
Phase 1) Environment Characterization



- Action performed (e.g., send STUN request to retrieve the subscriber GRA)
- Data retrieved (e.g., the subscriber GRA)
- Test performed (e.g., is the GRA configured on the Service Demarcation point)
- Conclusion stop block (i.e., NAT444 in the ISP, no NAT444 in the ISP or inconclusive)

Phase 2) NAT444 Discovery

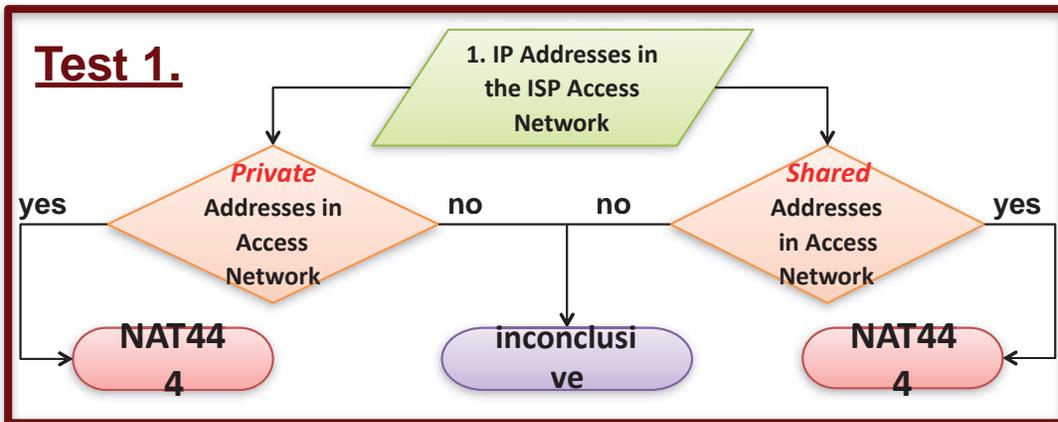
Environment Characterization



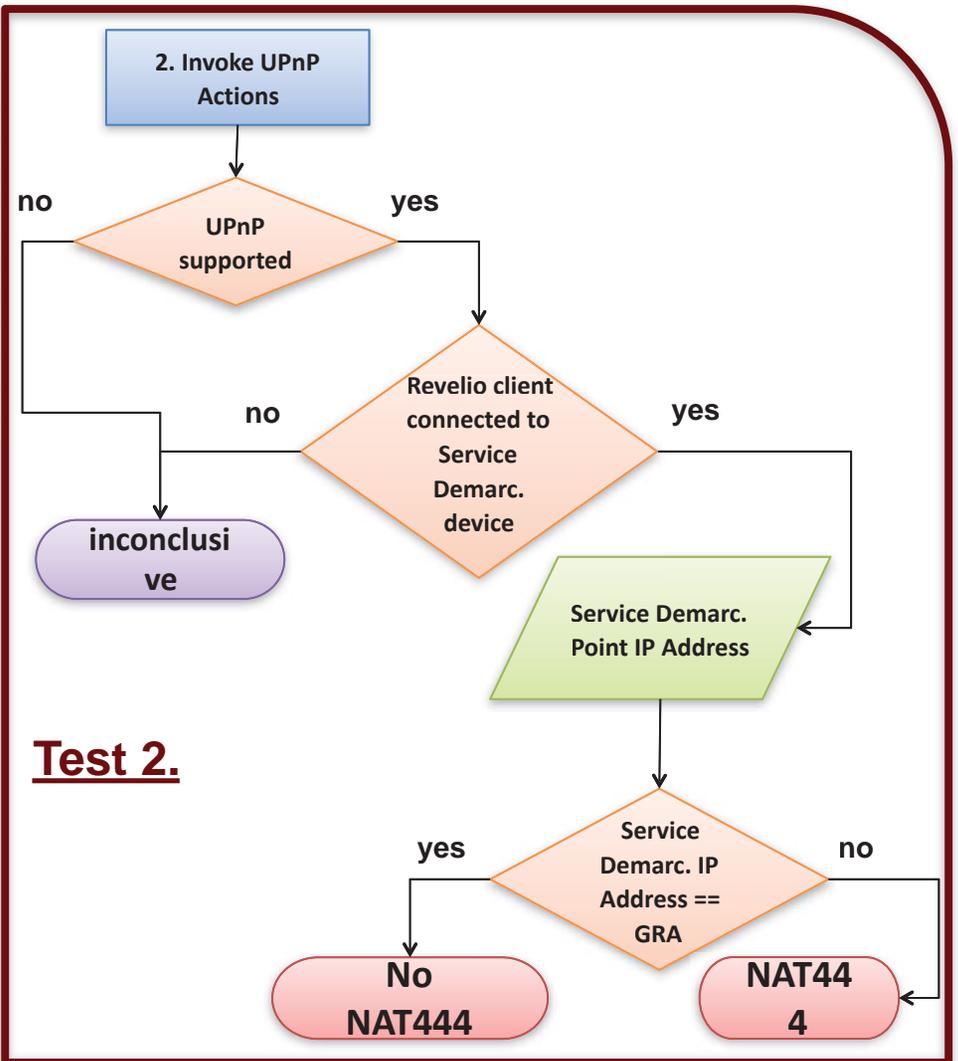
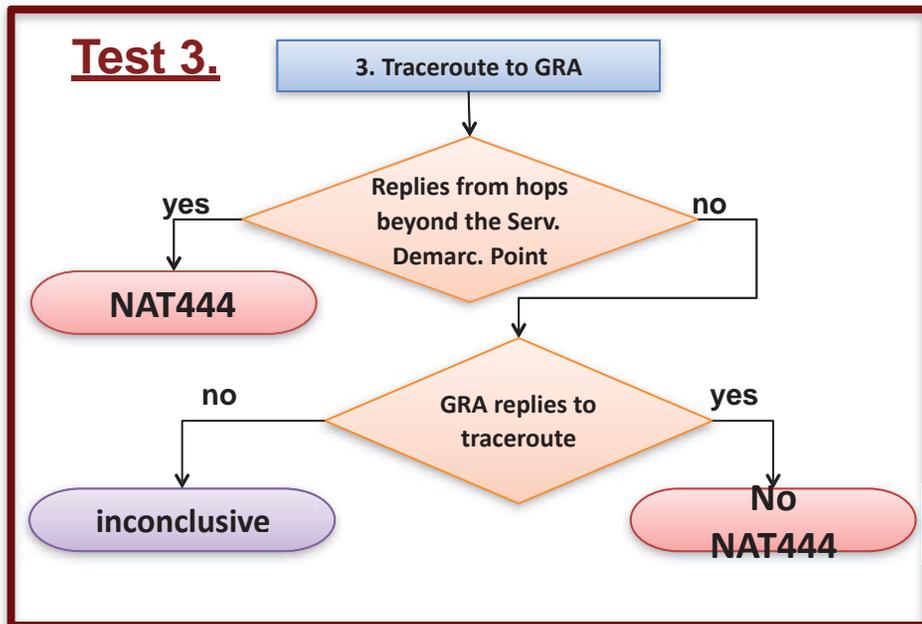
- This phase aims to determine:
 - **Test 1:** The GRA of the subscriber running the Revelio client
 - **Test 2:** Whether the subscriber is behind at least one level of NAT (i.e., the CPE performs the NAT function)
 - **Test 3:** Which is the position of the Revelio client related to the Service Demarc. Device (i.e., the position of the access link relative to the Revelio client)

NAT444 Discovery

Test 1.



Test 3.



Conclusions

- We propose *NAT Revelio* to detect the presence of NAT444 solutions in the ISP
- Some of the tests might fail at times, depending on the network we test (e.g., traceroute not working, CPE does not support UPnP)
- In case of conflicting results from different tests, we conclude an overall negative result for NAT444 in the ISP
- Thus, we do not categorically detect a NAT444 solution, but we determine the likelihood that there is one in the ISP, based on the analysis of the results of all the different tests we implement

Proposed Timeline

- Deploy tests on the MBA platform in Feb/March 2016
- Each run of the test suite takes ~2 days. Collect and analyze data from first run, validate results, tweak tests as necessary.
- Deploy periodically thereafter (monthly or quarterly) to enable study of evolution of CGN deployment.

