The Impact of IPv4/IPv6 Interworking on Lawful Intercept – a focus on CACmII reporting

Yi Liu, Scott Sheppard and Jennifer Joy
ATT Chief Security Office (CSO)
ATT Labs

Introduction of IPv6 and Transition Mechanisms to IASPs' Broadband Services

IPv6 address is introduced as a result of IPv4 address exhaust.

Due to the size of the Internet, it is not possible to migrate IPv4 addresses to IPv6 addresses in a synchronized manner. In fact, some IPv4 addresses may never change. Therefore, IPv6 and IPv4 will **co-exist** on the Internet for a long period of time.

This makes the support of **interworking** between IPv4 and IPv6 end points a must during the transition period. An IASP[1] should enable their customers using either protocol version to establish a connection to each other.

[1] IASP: Internet Access Service Provider (ATIS – 1000013.2007)

Impacts on Lawful Intercept

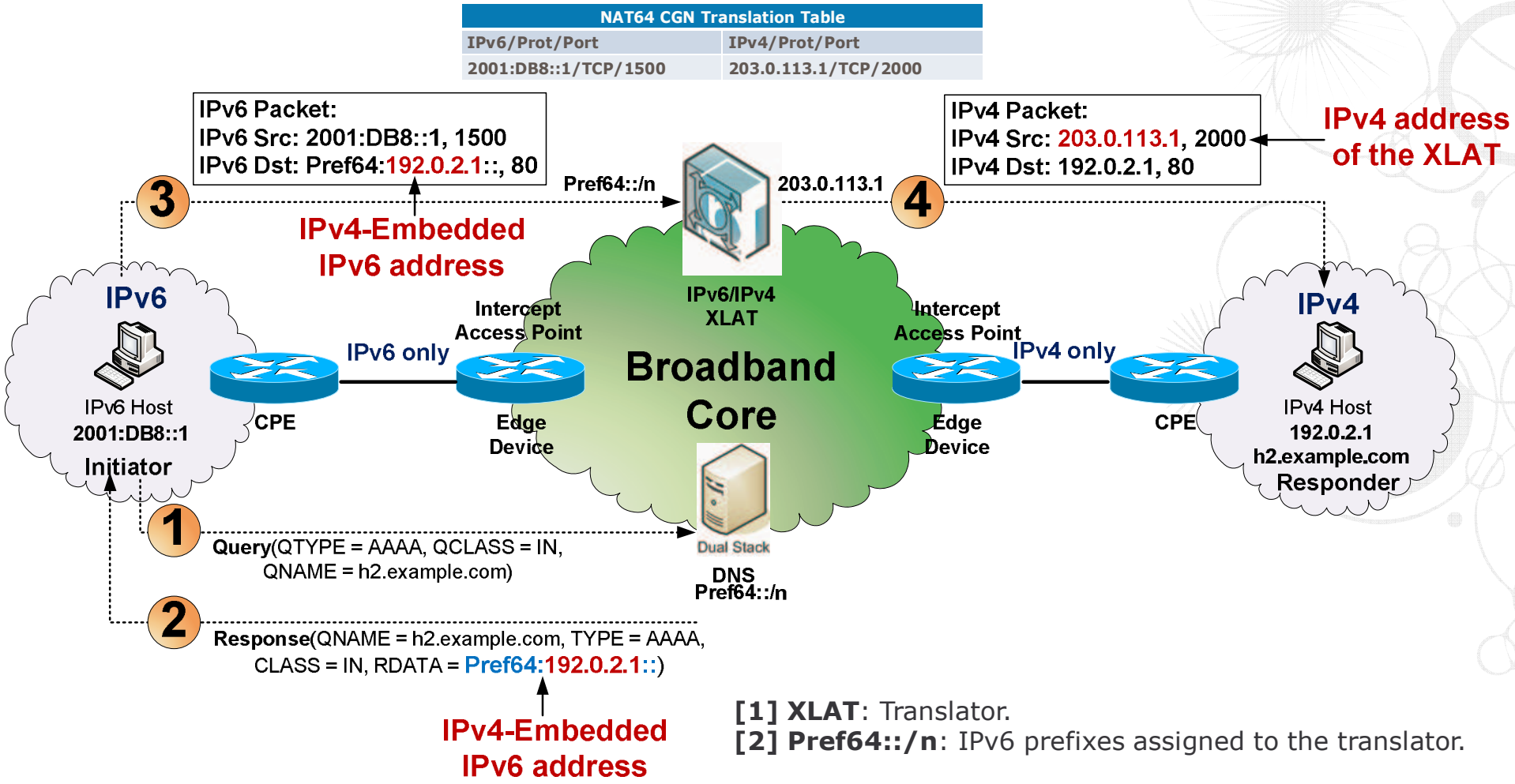
As a result of the introduction of the IPv4/IPv6 interworking scenarios, the end-to-end Lawful Intercept model is **disrupted**. For reporting **CACmII**[1], IASPs are faced with the technical challenge to best **restore and report** the original traffic characteristics of the target under surveillance (e.g., IASPs must report source and destination IP address and ports) which are **altered and/or hidden** by the transition mechanisms.

This presentation provides an impact analysis of the following transition mechanisms on the reporting of **CACmII**[1]. It also identifies possible solutions and open questions for each solution. The goal of the presentation is to stimulate effective brainstorming on the topic.

1. Integrated DNS64 and NAT64
2. DS-Lite (a combination of IPv4-in-IPv6 tunneling and CGN)

[1] CACmII: Content-Associated Communications Identifying Information (ATIS – 1000013.2007)

An Overview of Integrated DNS64 and NAT64



[1] XLAT: Translator.
[2] Pref64::/n: IPv6 prefixes assigned to the translator.

Integrated DNS64 and NAT64 – The Problem Statement (1/2)

The DNS64/NAT64 translation mechanism **disrupts** the end-to-end Lawful Intercept model and **alters** the original Source and Destination IP address of the communication session.

Intercept Subject	CACmII Fields	The original headers (end-to-end)	The altered headers (disrupted by the translator)
IPv6 host (the Initiator)	Source IP	2001:DB8::1	
	Destination IP	192.0.2.1	Pref64:192.0.2.1:: (altered by DNS64)
IPv4 host (the Responder)	Source IP	2001:DB8::1	203.0.113.1 (altered by NAT64)
	Destination IP	192.0.2.1	

Integrated DNS64 and NAT64 – The Problem Statement (2/2)

The IPv4/IPv6 interworking scenario involves hosts of both IP versions in one communication session. This requires reporting headers of **both IP versions** in the same CACmII message, which is **not allowed** by the standards.

T1.IAS (with Supplement A) only allows reporting headers of the same IP version in the same CACmII message. The standards are steps behind the industry evolution.

Integrated DNS64 and NAT64 – The Possible Solutions (1/2)

Option 1: IASPs do the job

The ability to report CACmII in a real-time fashion should not be compromised by the following:

1. Restore the IPv4 address from the DNS64 synthesized IPv6 address by stripping off the Pref64::/n.

   Pref64:192.0.2.1:: → 192.0.2.1

2. Trace back the IPv6 address from the translated IPv4 address given a source port and a timestamp (Traceability), by consulting the translation table or logs.

   203.0.113.1 (with a source port and a timestamp) → 2001:DB8::1

3. Represent the IPv4 address in the IPv4-Mapped IPv6 Address (RFC 4291) and report both source and destination IP address in IPv6 in the CACmII.

   192.0.2.1 → ::FFFF:192.0.2.1

Integrated DNS64 and NAT64 – The Possible Solutions (2/2)

Option 2: LEAs do the job with IASPs' assistance:

1. LEAs restore the IPv4 address with the definition rule of Pref64::/n supplied by the IASP.

   Pref64:192.0.2.1:: → 192.0.2.1

Integrated DNS64 and NAT64 – Open Questions (1/2)

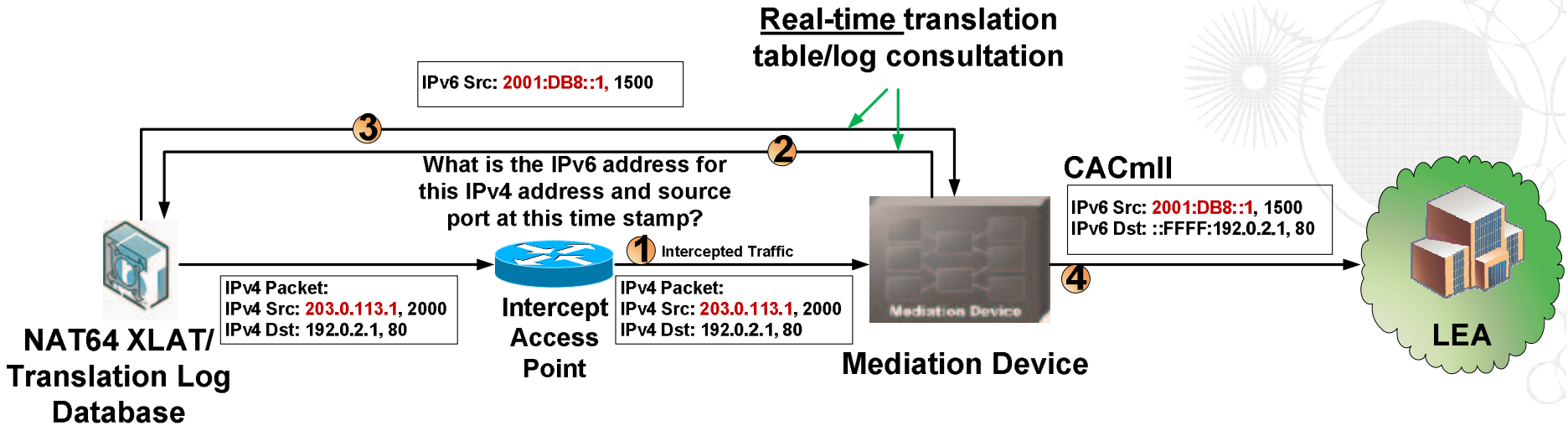
While the possible solutions seemed intuitive there are open questions worth consideration:

1. Is the IPv4-Mapped IPv6 Address understood by LEAs?

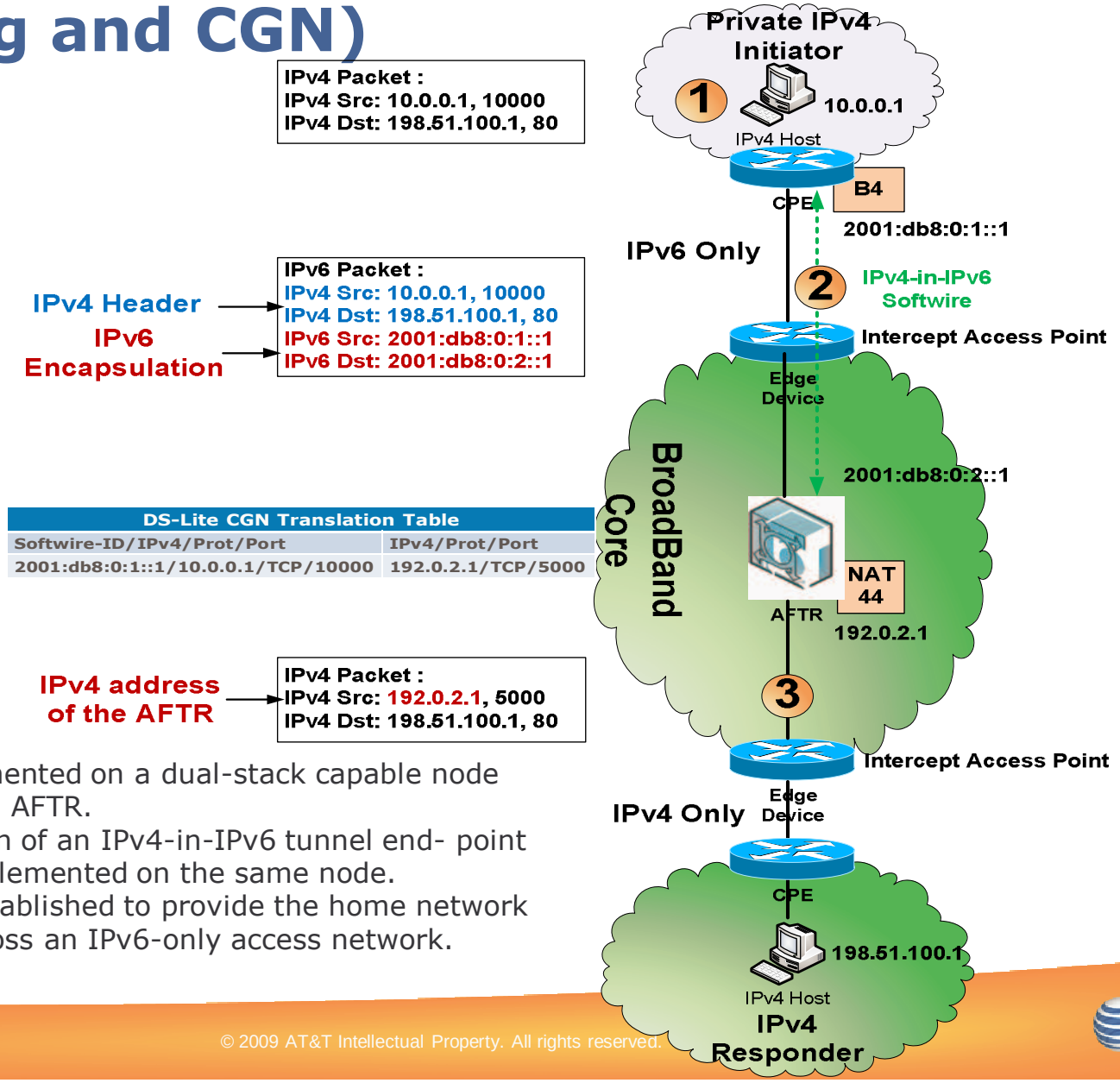
2. Are LEAs willing to restore the IPv4 address by themselves?

Integrated DNS64 and NAT64 – Open Questions (2/2)

3. Is the real-time trace-back (retrieval of the IPv6 address from the translated IPv4 address given a source port and a timestamp) technically feasible? Is the high cost justified?



An Overview of DS-Lite (a combination of Tunneling and CGN)



[1] B4: A function implemented on a dual-stack capable node that creates a tunnel to an AFTR.
[2]AFTR: The combination of an IPv4-in-IPv6 tunnel end- point and an IPv4-IPv4 NAT implemented on the same node.
[3]Softwire: A tunnel established to provide the home network with IPv4 connectivity across an IPv6-only access network.

at&t

DS-Lite – The Problem Statement

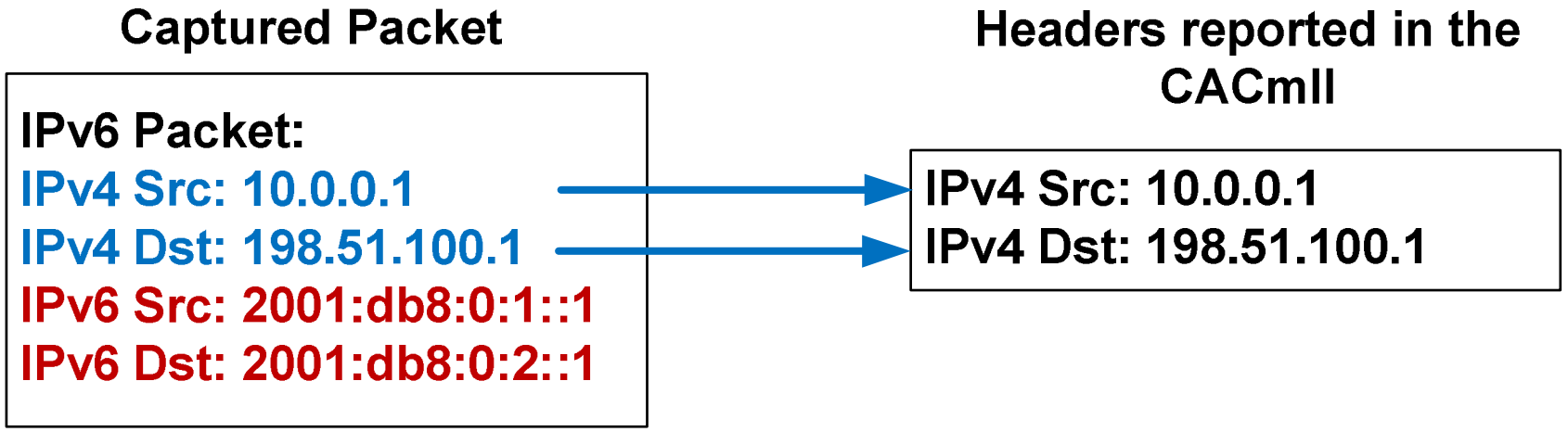
1. The intercepted traffic (IPv4 packet) is **hidden** (encapsulated) in the IPv4-in-IPv6 Softwire.
2. CGN (NAT44) **alters** the original source IP address of the communication session.

Intercept Subject	CACmII Fields	The original headers (end-to-end)	The altered headers (disrupted by the translator/NAT)
IPv4 host (the Initiator)	Source IP	10.0.0.1	2001:db8:0:1::1 (IPv4 address is hidden behind the tunnel endpoint)
	Destination IP	198.51.100.1	2001:db8:0:2::1 (IPv4 address is hidden behind the tunnel endpoint)
IPv4 host (the Responder)	Source IP	10.0.0.1	192.0.2.1 (altered by NAT44)
	Destination IP	198.51.100.1	

DS-Lite – The Possible Solutions (1/2)

Option 1:

De-capsulate the Softwire to restore and report the IPv4 headers (the initiator is private IPv4) in the CACmII message.

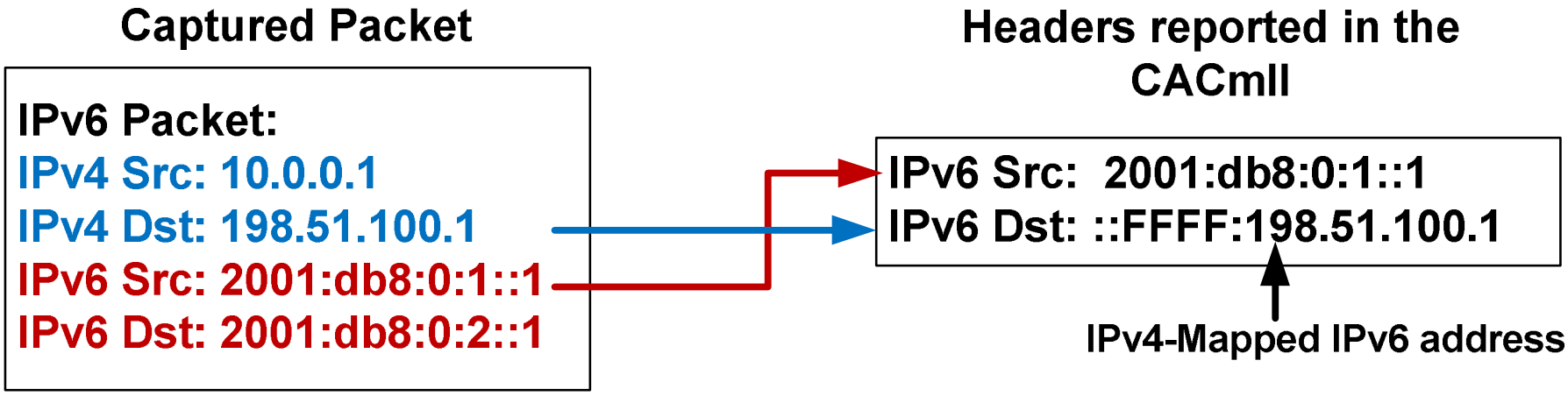


at&t

DS-Lite – The Possible Solutions (2/2)

Option 2:

Generate the CACmII message based on a combination of IPv4 and IPv6 headers and represent the IPv4 address in the IPv4-mapped IPv6 address.



at&t

DS–Lite – Open Questions

While the possible solutions seemed intuitive there are open questions worth consideration:

1. Is the real-time trace-back technically feasible? Is the high cost justified?
2. Option 1
   - Is reporting IP headers for private end points in Enterprises required by CALEA? Are IASPs willing to take on the obligation?
   - Will reporting of IPv4 address lead to confusion when the subject is targeted by IPv6 address?
3. Option 2
   - Is the cost required by the complex mediation process justified?
   - Is the IPv4-Mapped IPv6 Address understood by LEAs?

Concluding Remarks

An in-depth impact analysis of the IPv4/IPv6 interworking scenarios on Lawful Intercept CACmII reporting enables both the Law Enforcement Agencies and the Industry to reach a middle ground between what information is required to be reported and what can be achieved by the technology within reasonable cost.

The impact analysis also drives and provides valuable input to formal standards processes (ETSI, ATIS, Etc).

at&t

Thank You!