NAT traversal for LISP

draft-ietf-lisp-nat-traversal-00

L. Iannone (Ed.)

IETF 124 – Montreal

Since IETF 122: Adopted by WG

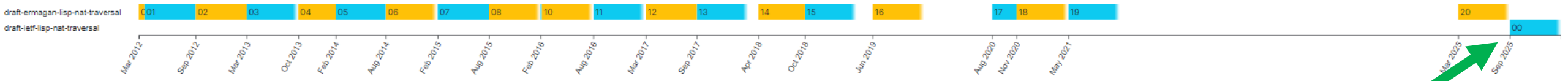
NAT traversal for LISP

draft-ietf-lisp-nat-traversal-00

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00



draft-ietf-lisp-nat-traversal-00.txt
September 2025
Document adopted and renamed

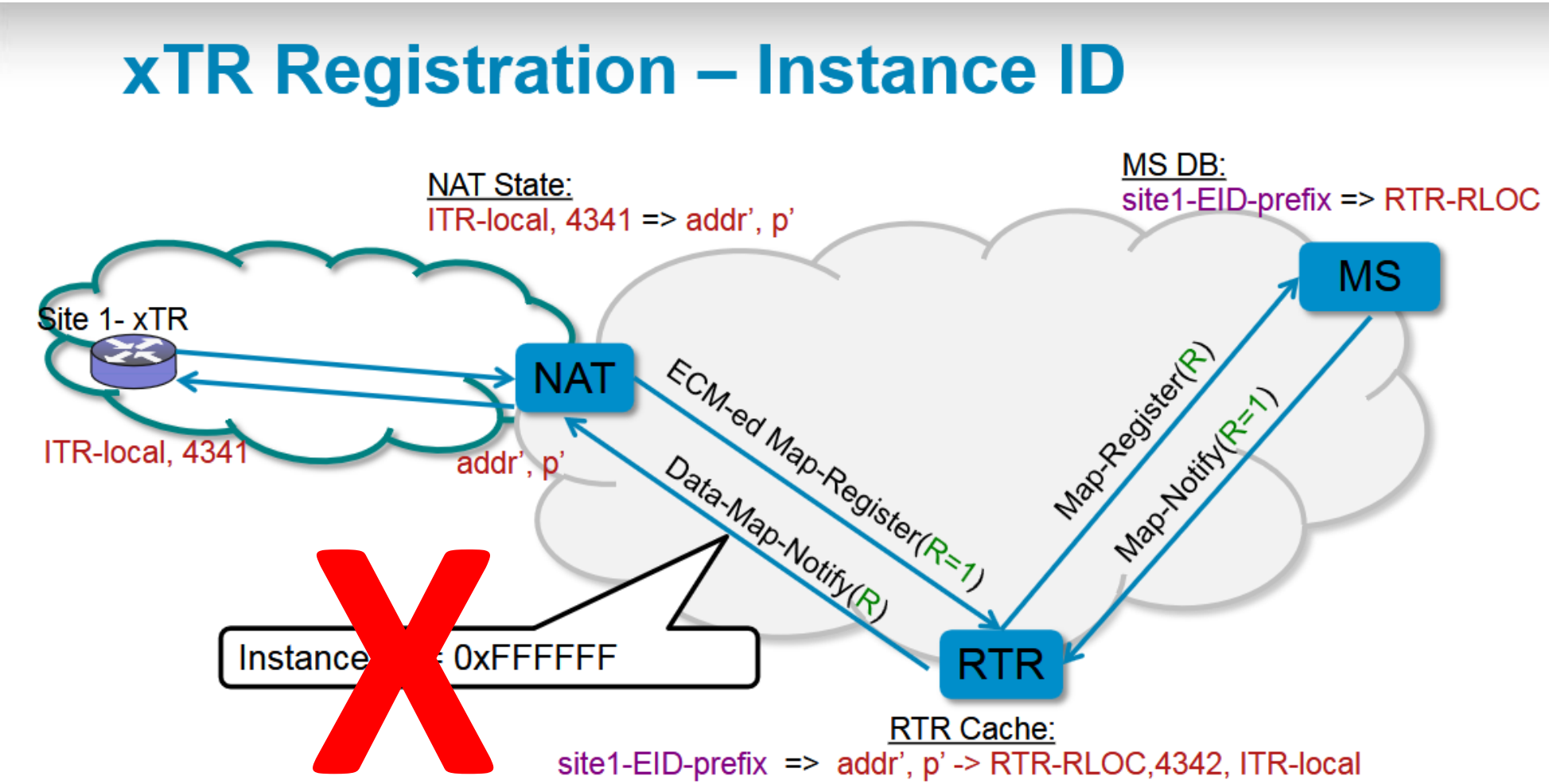
Structure stable

Table of Contents

Table of Contents

- A lot of typos' correction
- Added backward compatibility discussion

Recall: Instance ID to identify Data-Map Notify

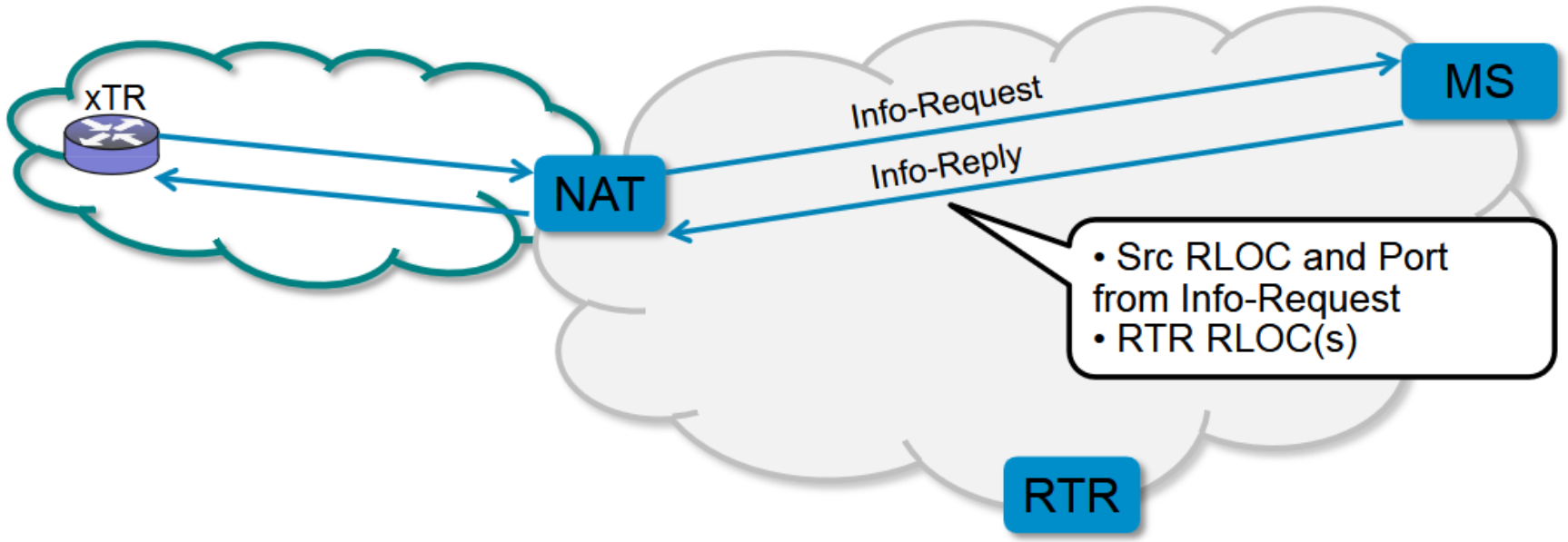


- Instance ID 0xFFFFFF is used to identify a LISP control packet encapsulated in a LISP data header

- Data-Map-Notify is a Map-Notify encapsulated in a LISP Data plane header (port 4341)
- The use of the IID is a "**shortcut**" to identify this type of packets and has **been dropped**
- Normal decapsulation and packet dispatch work and is also more secure because the inner packet goes through existing filters

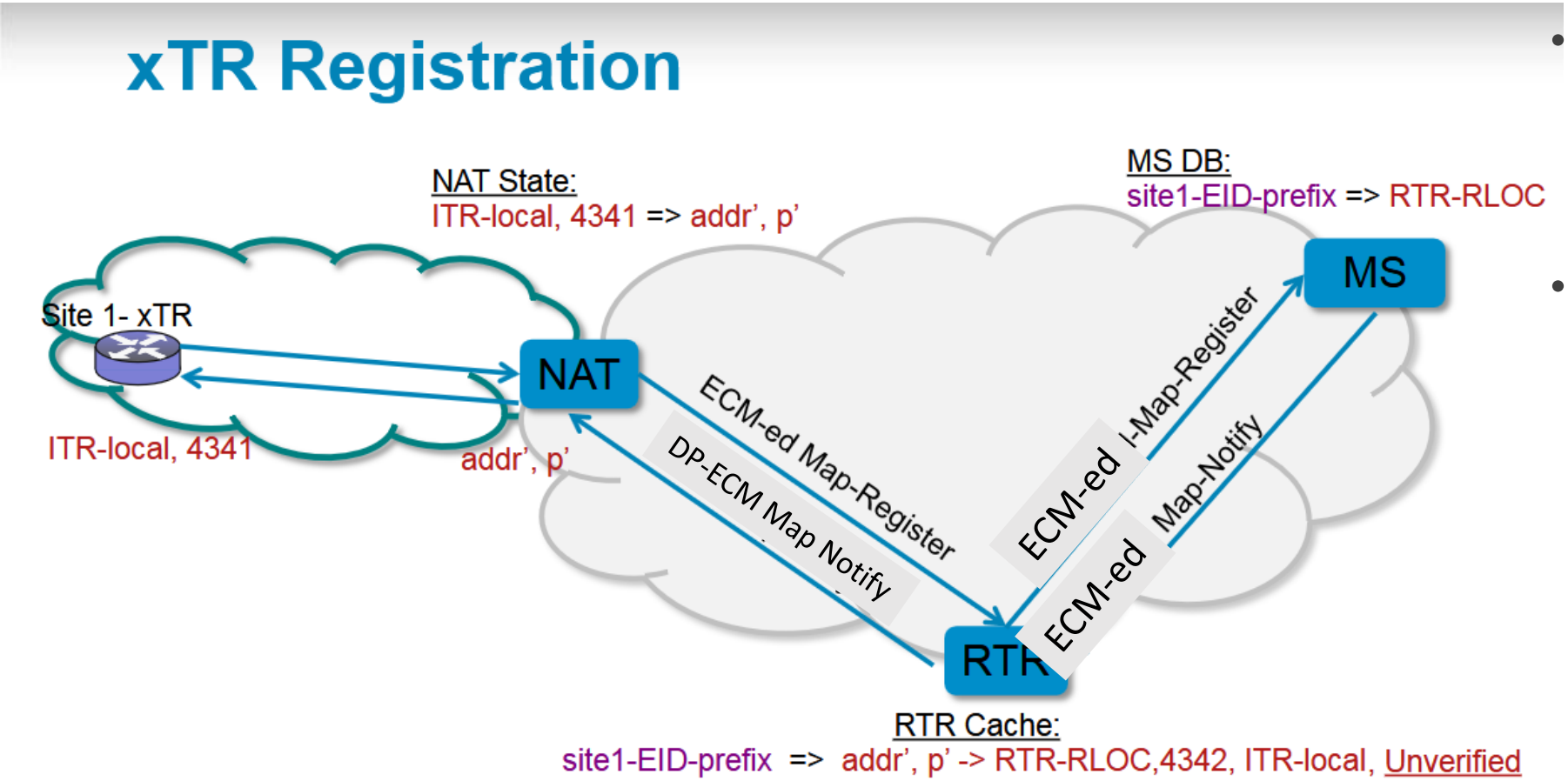
Recall: NAT Traversal Security (I)

NAT Discovery



- Info-Request and Info-Reply messages have similar header structure of Map-Register and Map-Notify, as such authentication and integrity can be performed in the same way (Section 5.6 of [RFC9301])

Recall: NAT Traversal Security (I)



- **DP-ECM Map-Notify:** Map-Notify in an ECM encapsulated with a Data Plane LISP header
- All other messages were already defined as ECM messages

- **Map-Register and Map-Notify** verified for authentication and integrity using pre-shared key **between the xTR and the Map-Server** as for [RFC9301]
- For **authentication and integrity protection of the RTR**, the **ECM LISP-SEC Extensions** (Sectior 6.1 of [RFC9303]) are used, employing two different pre-shared keys, one between the RTR and the ETR and one between the RTR and the Map-Server.

Backward Compatibility

9. IANA Considerations

9. Backward Compatibility with early version of this document

Early versions of this document did not make use of DP-ECM encapsulation for the Map-Notify messages from RTRs to xTRs. Instead, a simple LISP Data plane encapsulation was used, which was marked with the IID field set to 0xFFFFFF so to hand over the packet directly from the LISP data plane to the LISP control plane. However, these choice come with the following drawbacks:

* Without ECM encapsulation, the receiving xTR has no means to authenticate and verify the integrity of the message coming from RTR, since the inner Map-Notify only authenticates the Map-Server

* The use of the IID 0xFFFFFF as shortcut through the protocol stac may lead to skip security checks and may be considered as an attack vector. Decapsulating the LISP data plane packet and re-injecting it in the protocol stack, may appear less efficient but allows to make sure that the inner packet is checked against any security and/or filtering policy configured on the xTR.

Early versions of this document also used to put an additional 16-bits field at the end of the Info-Request message to mark the end of the message. Rationale was: If this AFI field is 0 nothing follows, if this field is set to 16387, then a NAT LCAF is present. However, such field is pointless, since the UDP header encapsulating the LISP control messages has a field indicating the length of the message.

For security reasons, as described in Section 8 the ECM encapsulation has been added in order to enable authetication of Map-Notify messages sent by RTRs to xTRs, the use of the 0xFFFFFF IID hasbeen also dropped, and Info-Request messages do not terminate with a null field.

Implementations using early versions of this document are not compatible with the current specifications. For security reasons it is RECOMMENDED to use implementations that support DP-ECM. New LISP NAT traversal deployments MUST use implementations that support DP-ECM Map-Notify messages.

10. IANA Considerations

- Introducing DP-ECM and its rationale
- Avoid using null fields
- For security reasons this document RECOMMENDS to use implementations with latest specs

Next Steps

- WG Last Call?

THANKS!