draft-ermagan-lisp-nat-traversal-00

Vina Ermagan, Dino Farinacci, Darrel Lewis, Fabio Maino, Jesper Skriver, Chris White

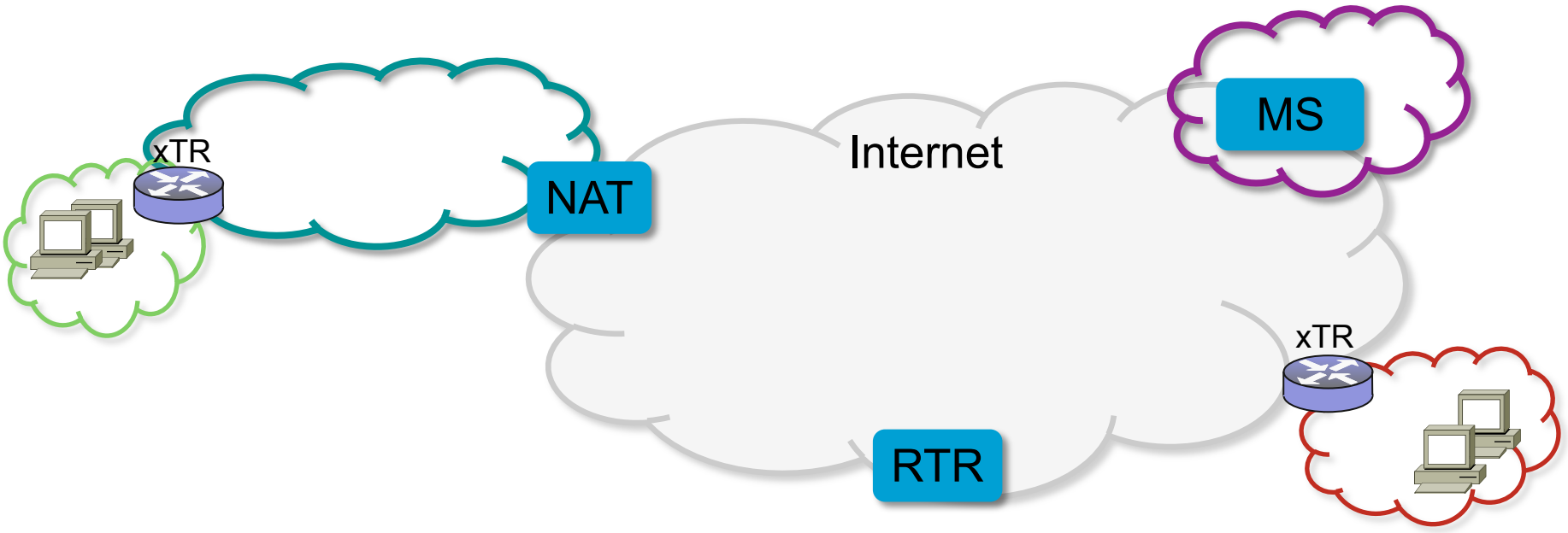
Presenter: Vina Ermagan

IETF 83, Paris – March 2012

Agenda

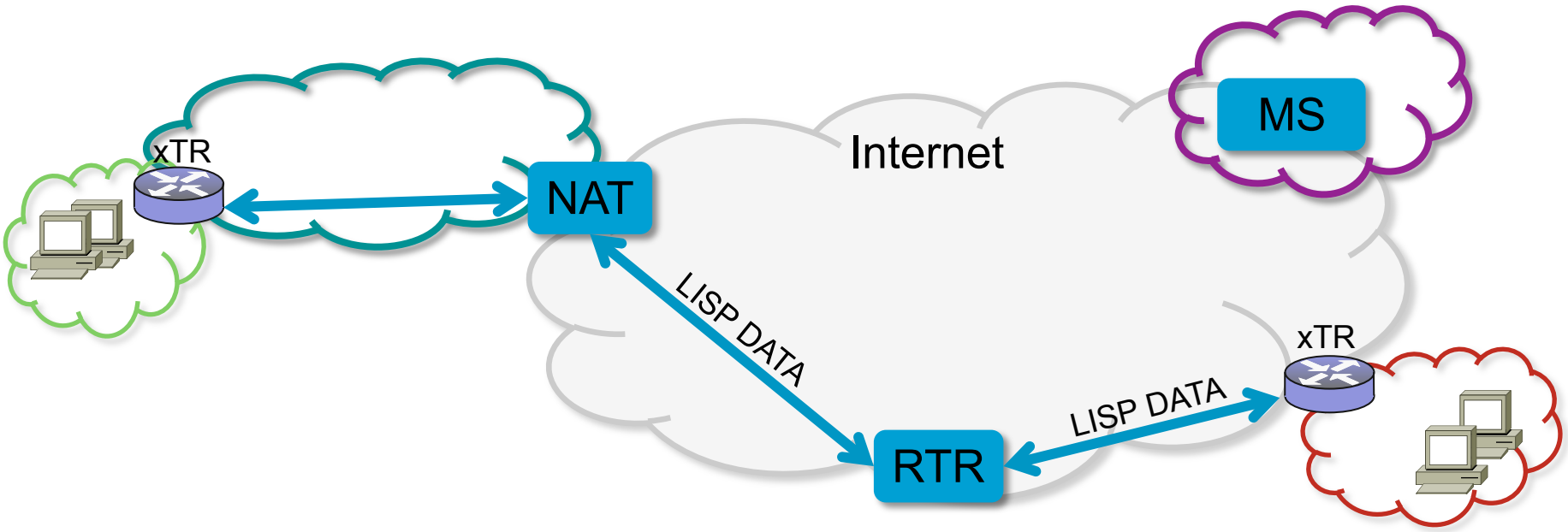
- Problem Overview and scope
- NAT Discovery
- xTR Registration
- Multiple xTRs behind the NAT
- Map-Request handling
- Data Flow
- Message formats
- Q&A

LISP NAT Traversal – Overview and Scope



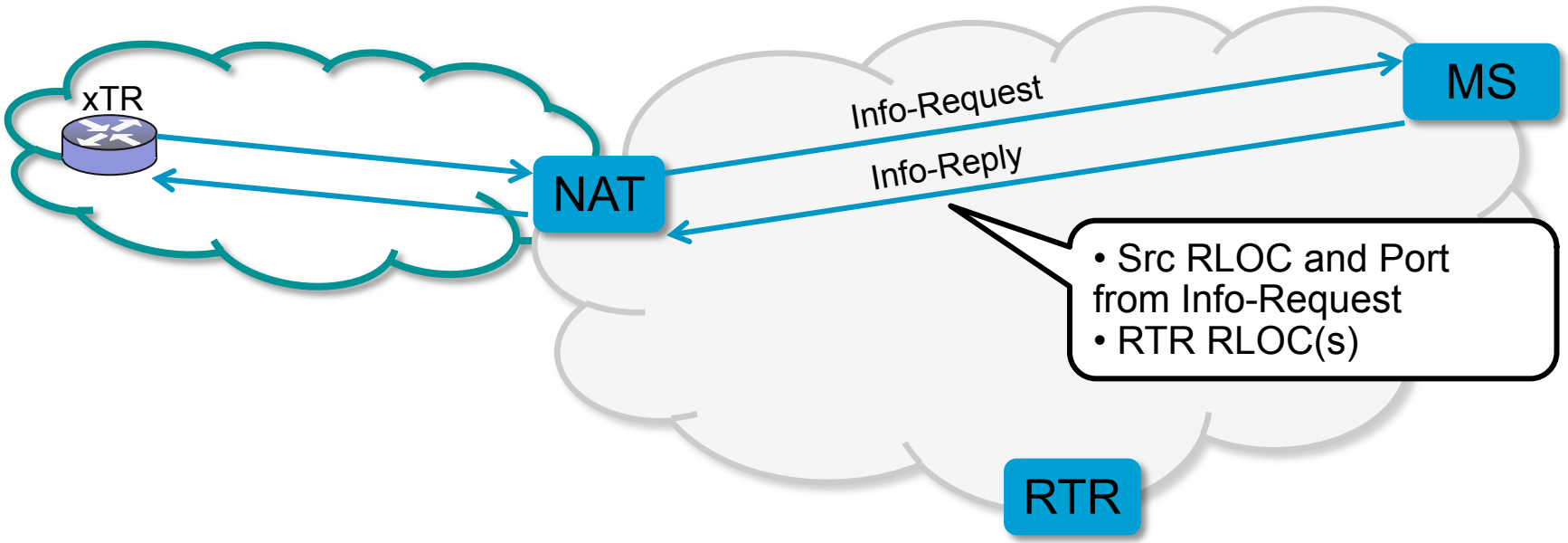
- LISP relies on the xTR being reachable at its RLOC and on ports 4341 and 4342, to receive LISP data and control traffic
- A NAT traversal mechanism is required to enable
  - NAT discovery
  - xTR reachability on port 4341
- Scope: NAT traversal for the deployments where xTR is behind a NAT but its Map-Server is on the public side of the NAT

LISP NAT Traversal - Overview



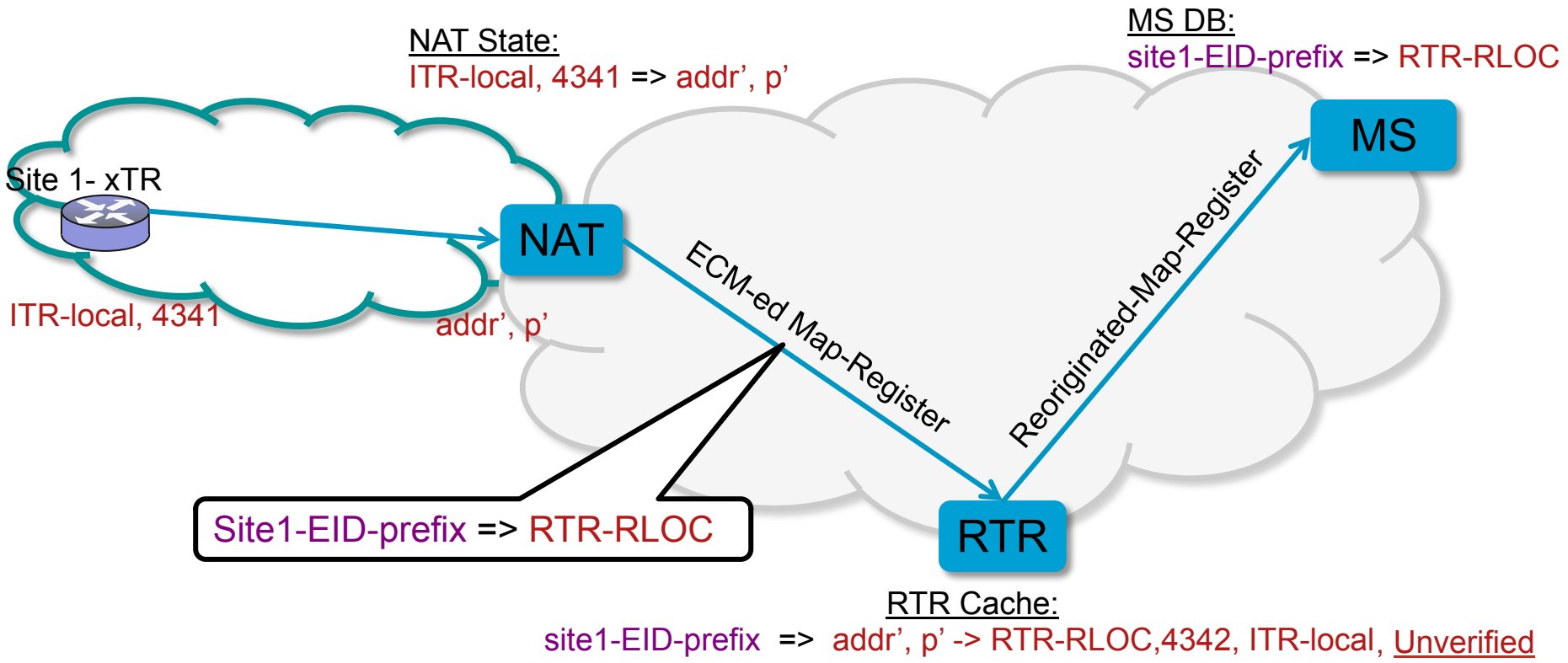
- RTR: Re-encapsulating Tunnel Router
- RTR acts as a data plane proxy for LISP data traffic to and from the xTR behind the NAT
- This enables maintaining the LISP Control plane and Data plane separation

NAT Discovery



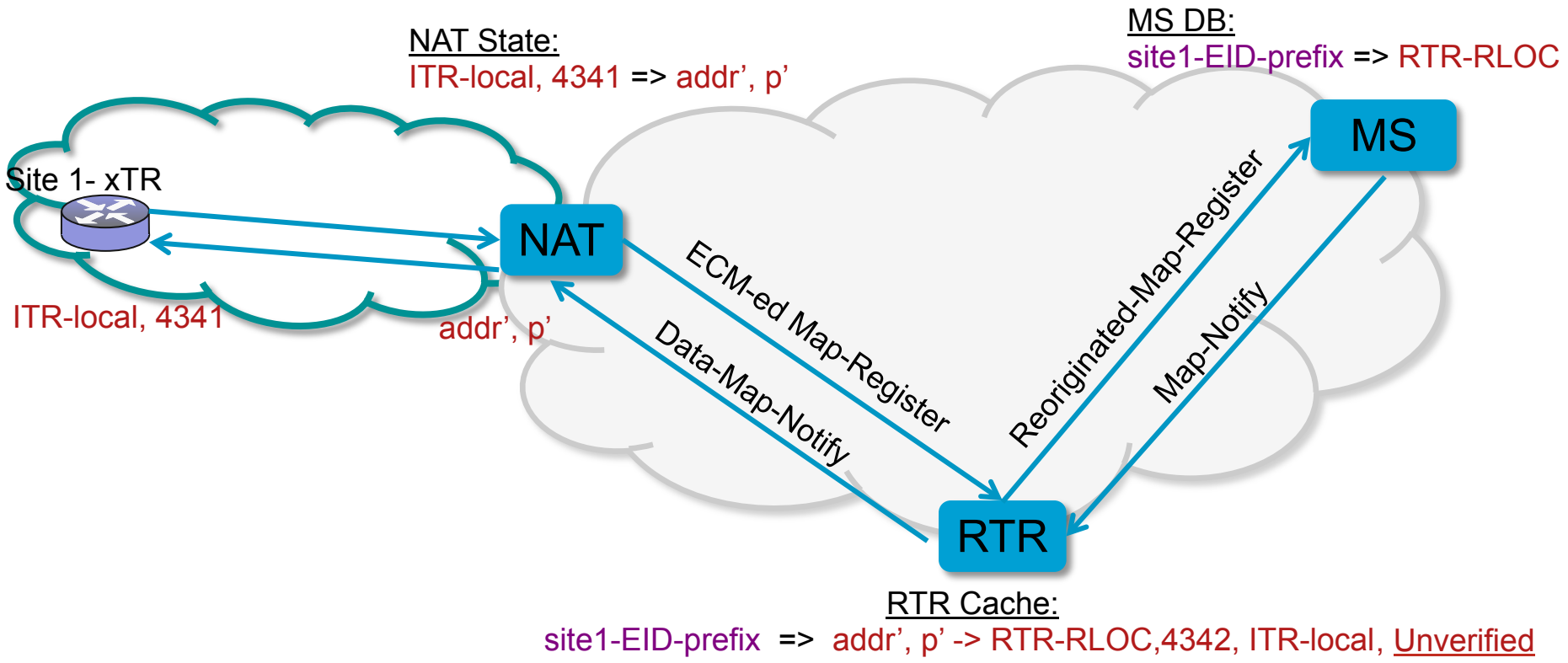
- xTR receives a new RLOC and sends Info-Request using the new RLOC to its Map-Server
- MS replies with an Info-Reply
- xTR compares the new RLOC and port with src RLOC and port from info-Reply to discover NAT device on the path
- If NAT exists, xTR picks one (or more) RTR RLOC from the Info-Reply and proceeds to Registration

xTR Registration



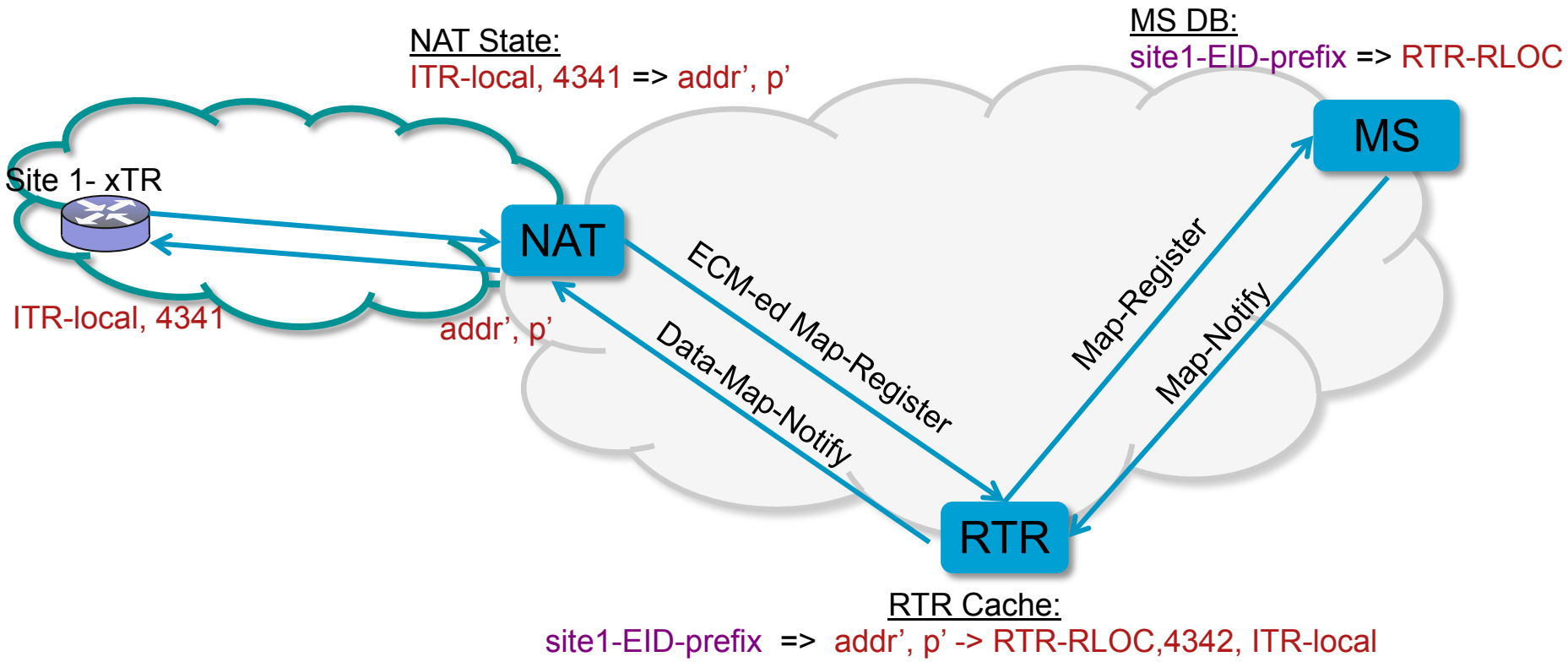
- Goals:
  - Register RTR-RLOC for site-1-EID-prefix in MS
  - RTR learn addr', p' associated with site1-EID-prefix
  - Setup required NAT state
- Avoid creating new security threats due to gleaning an RLOC

xTR Registration

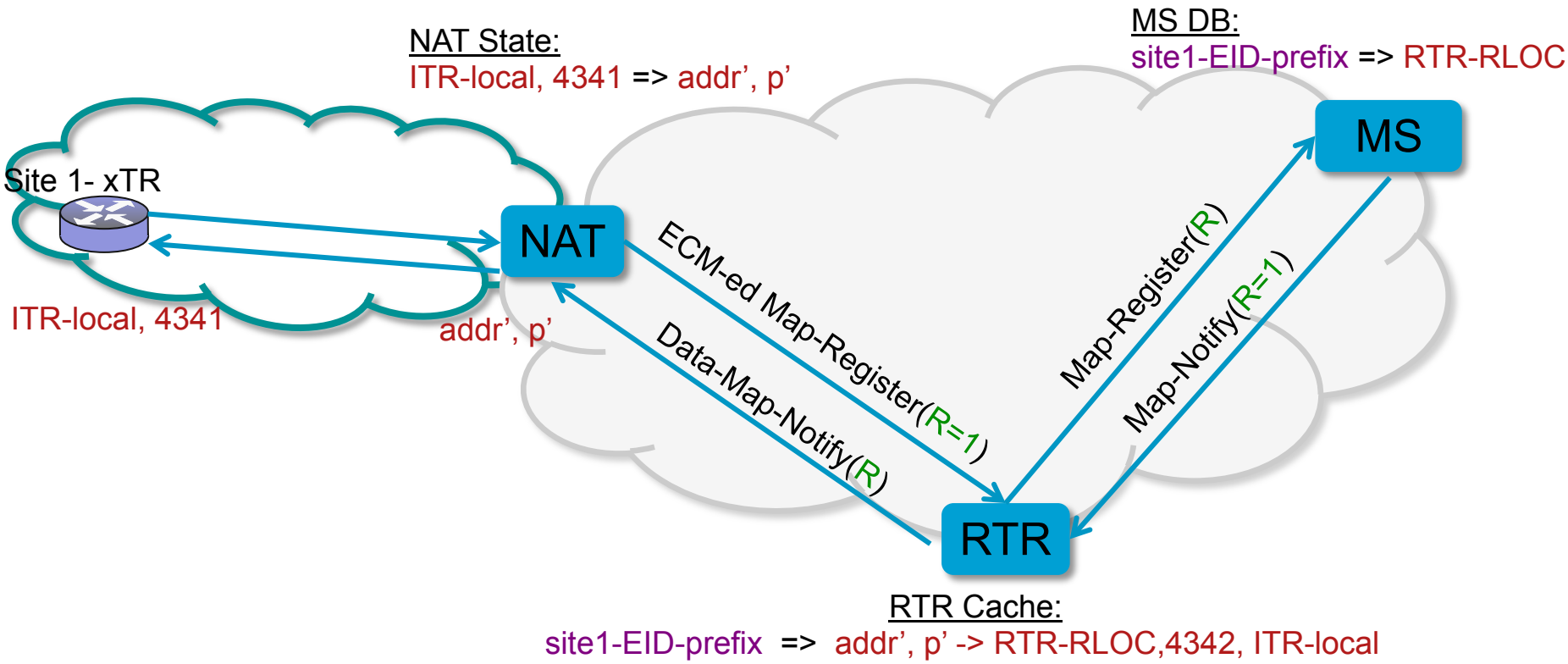


- Goals:
  - Register RTR-RLOC for site-1-EID-prefix in MS
  - RTR learn addr', p' associated with site1-EID-prefix
  - Setup required NAT state
- Avoid creating new security threats due to gleaning an RLOC

xTR Registration – R bit

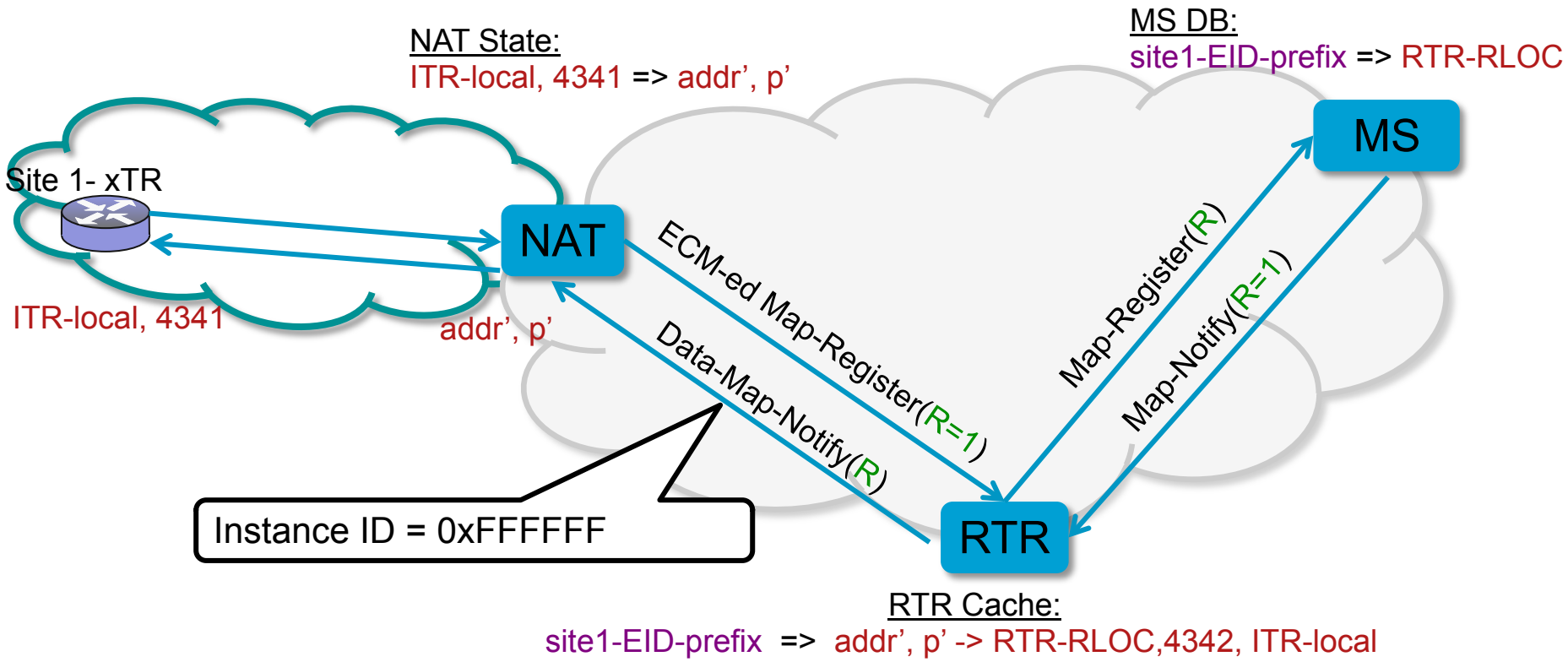


xTR Registration – R bit



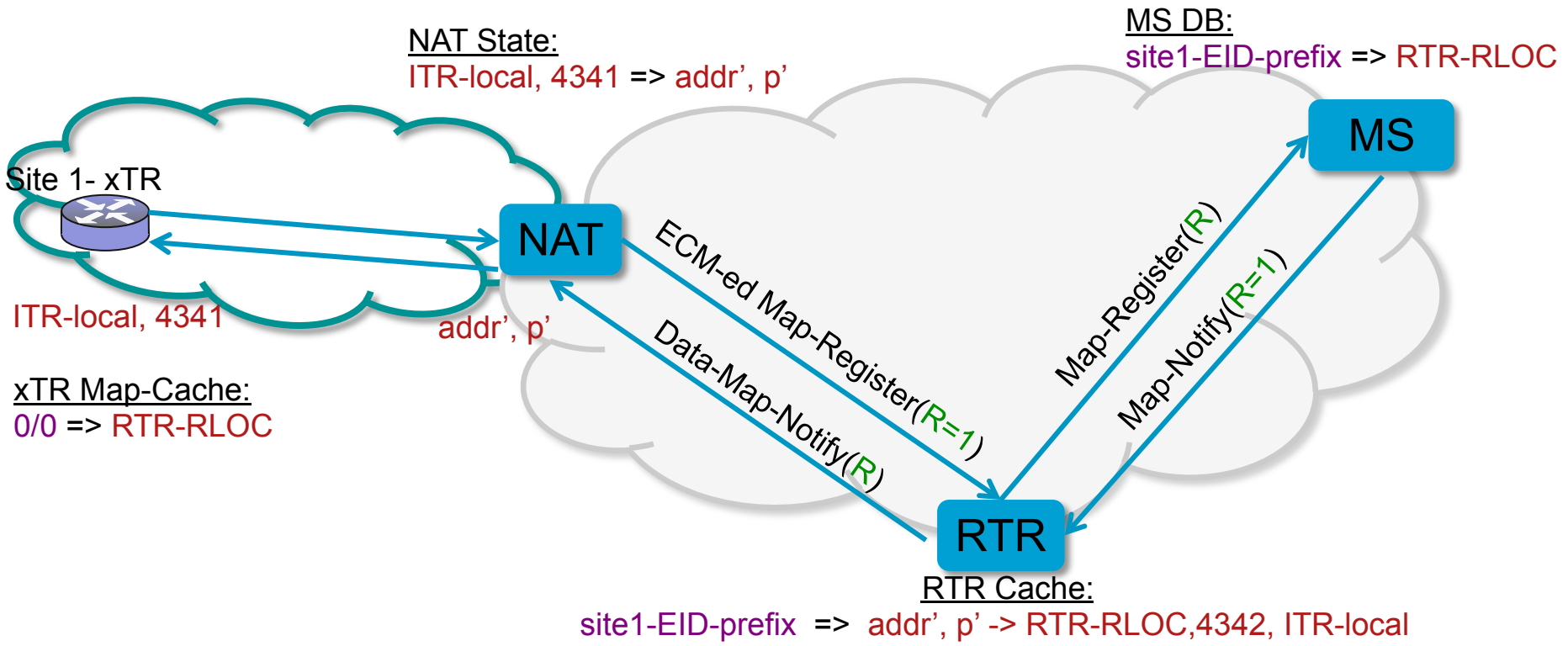
- Sending the Map-Register/Map-Notify through the RTR allows the RTR to verify the EID-prefix-to-RLOC mapping when caching.
- Map-Notify (R=1): MS-RTR Authentication Data is appended at the end of the Map-Notify
- RTR verifies the MS-RTR Auth. Data for integrity protection and origin authentication of Map-Notify

xTR Registration – Instance ID



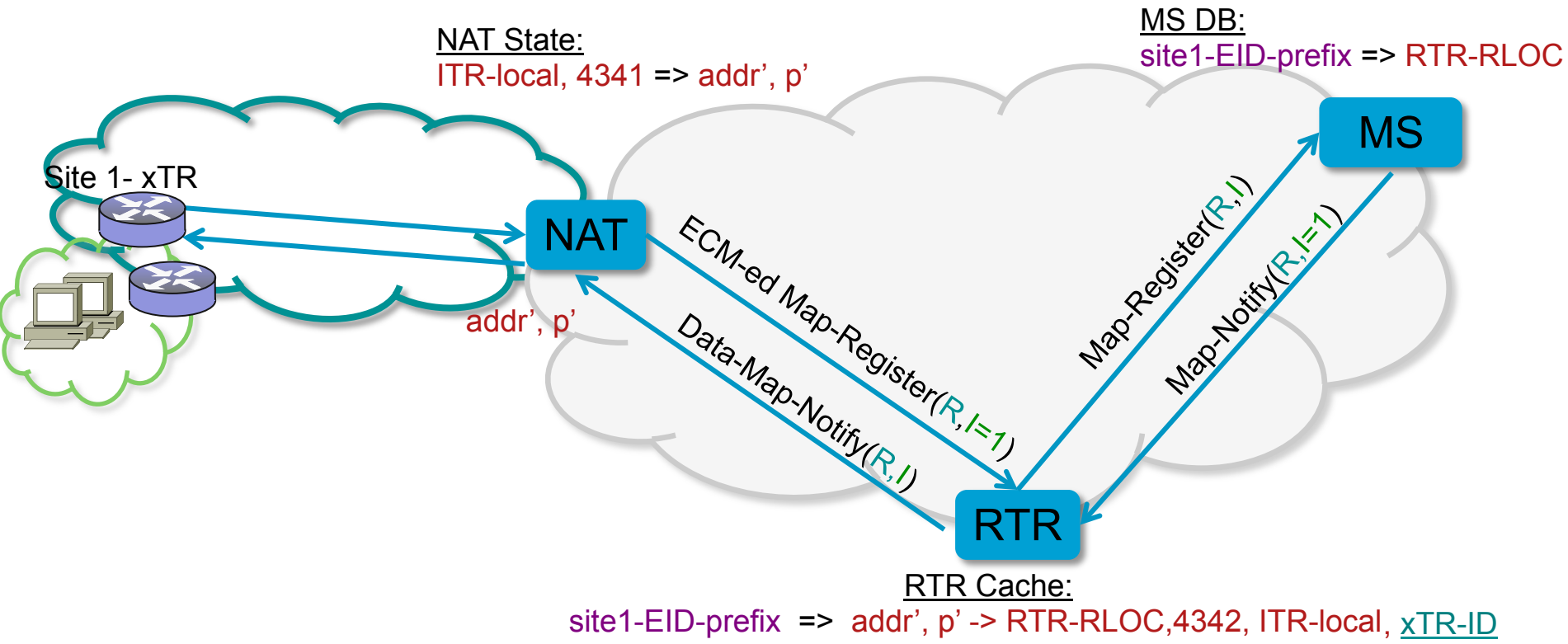
- Instance ID 0xFFFFFF is used to identify a LISP control packet encapsulated in a LISP data header

Map-Request Handling



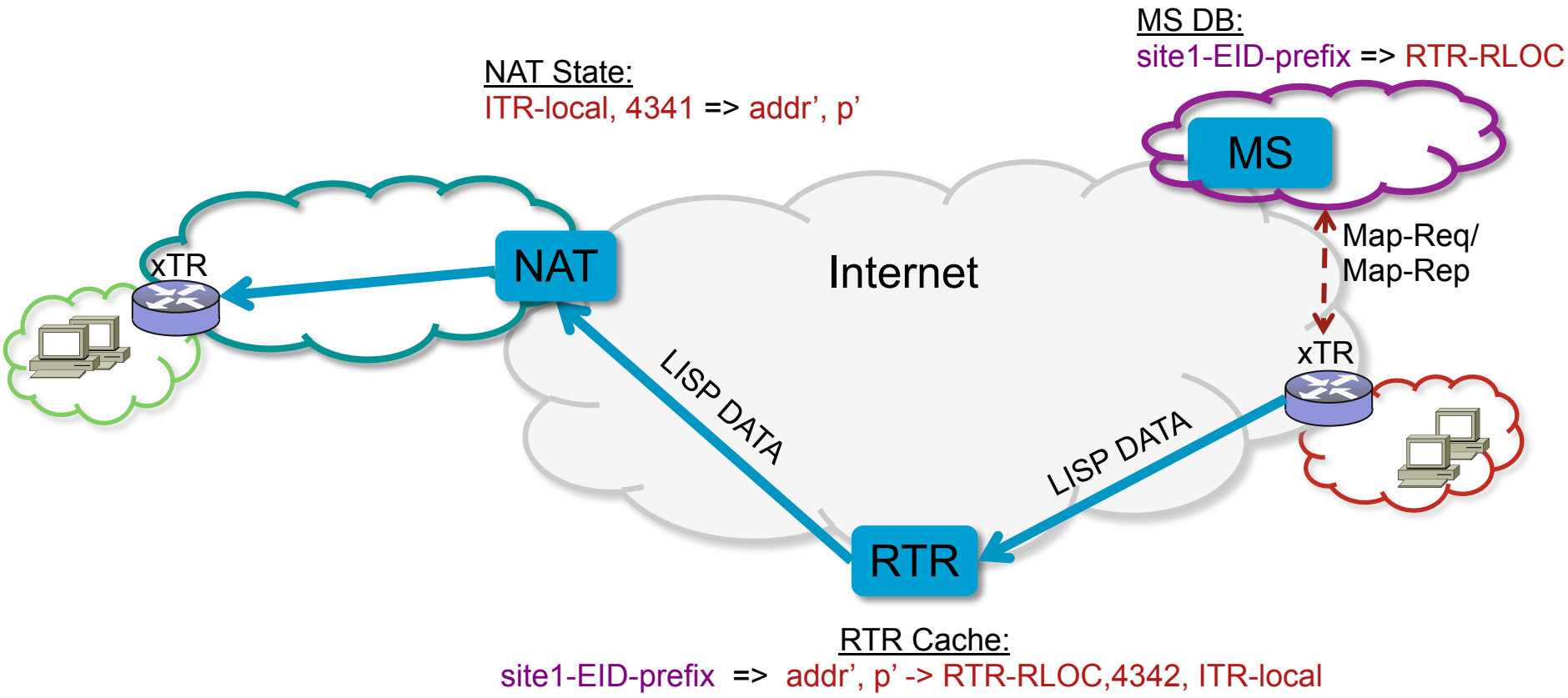
- By storing RTR-RLOC as default RLOC for data plane LISP traffic xTR encapsulates all LISP data packets to RTR
- By setting the proxy bit in Map-Register xTR can activate Map-Server Proxy Reply
- If proxy bit is not set in Map-Register: xTR periodically sends Info-Requests. MS encapsulates Map-Requests to xTR (not recommended)

xTR Registration – Multi xTR site

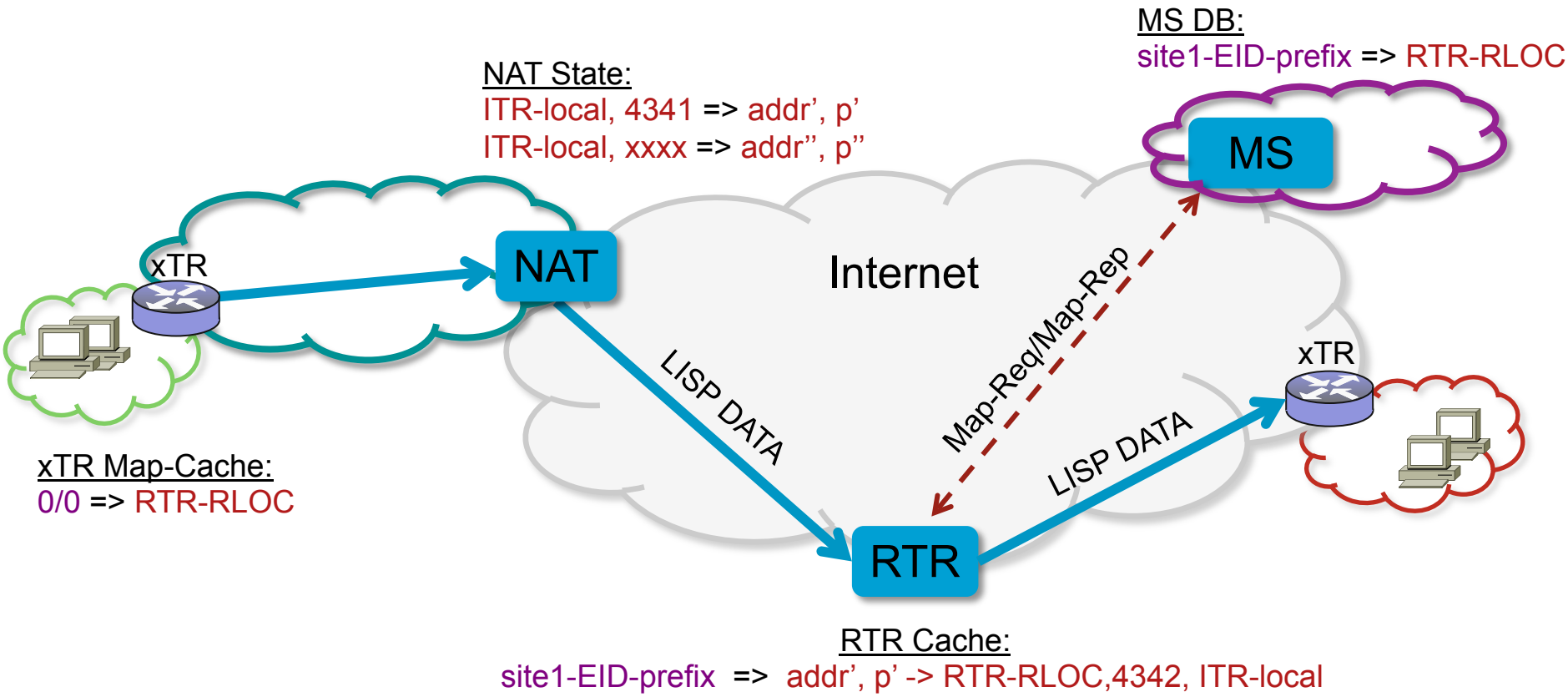


- xTR-ID: 128 bit xTR-ID is appended at the end of the Map-Register message, Map-Register (R=1, I=1):
- RTR, and MS cache xTR-ID.
- MS includes xTR-ID in Map-Notify messages
- RTR uses xTR-ID in Map-Notify to identify destination xTR

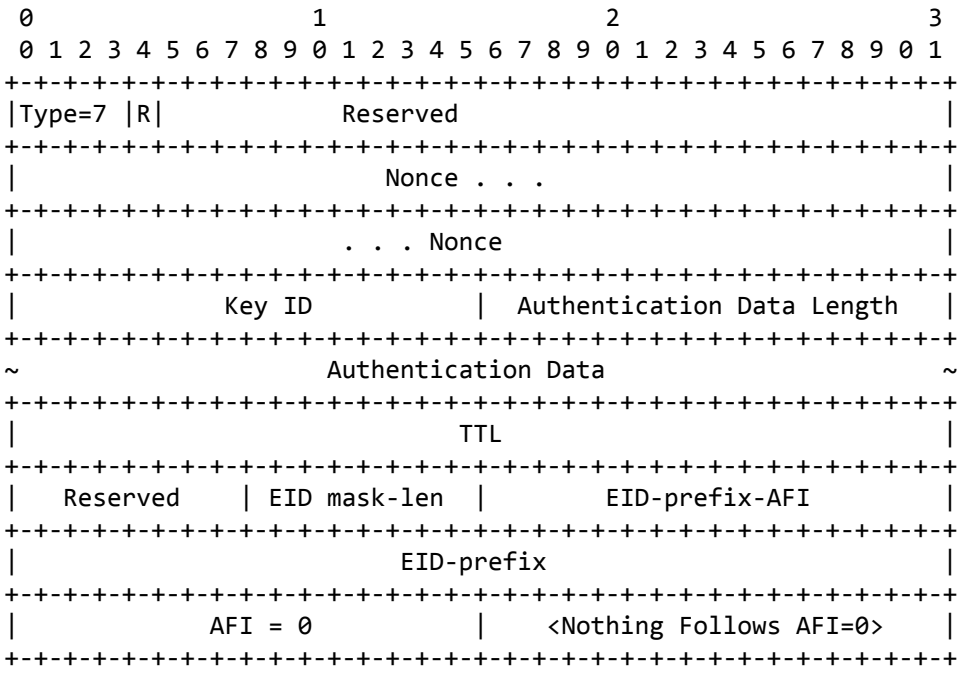
Data Flow I


MS DB:
site1-EID-prefix => RTR-RLOC
NAT State:
ITR-local, 4341 => addr', p'
MS
Map-Req/
Map-Rep
xTR
NAT
Internet
xTR
LISP DATA
LISP DATA
RTR
RTR Cache:
site1-EID-prefix => addr', p' -> RTR-RLOC,4342, ITR-local

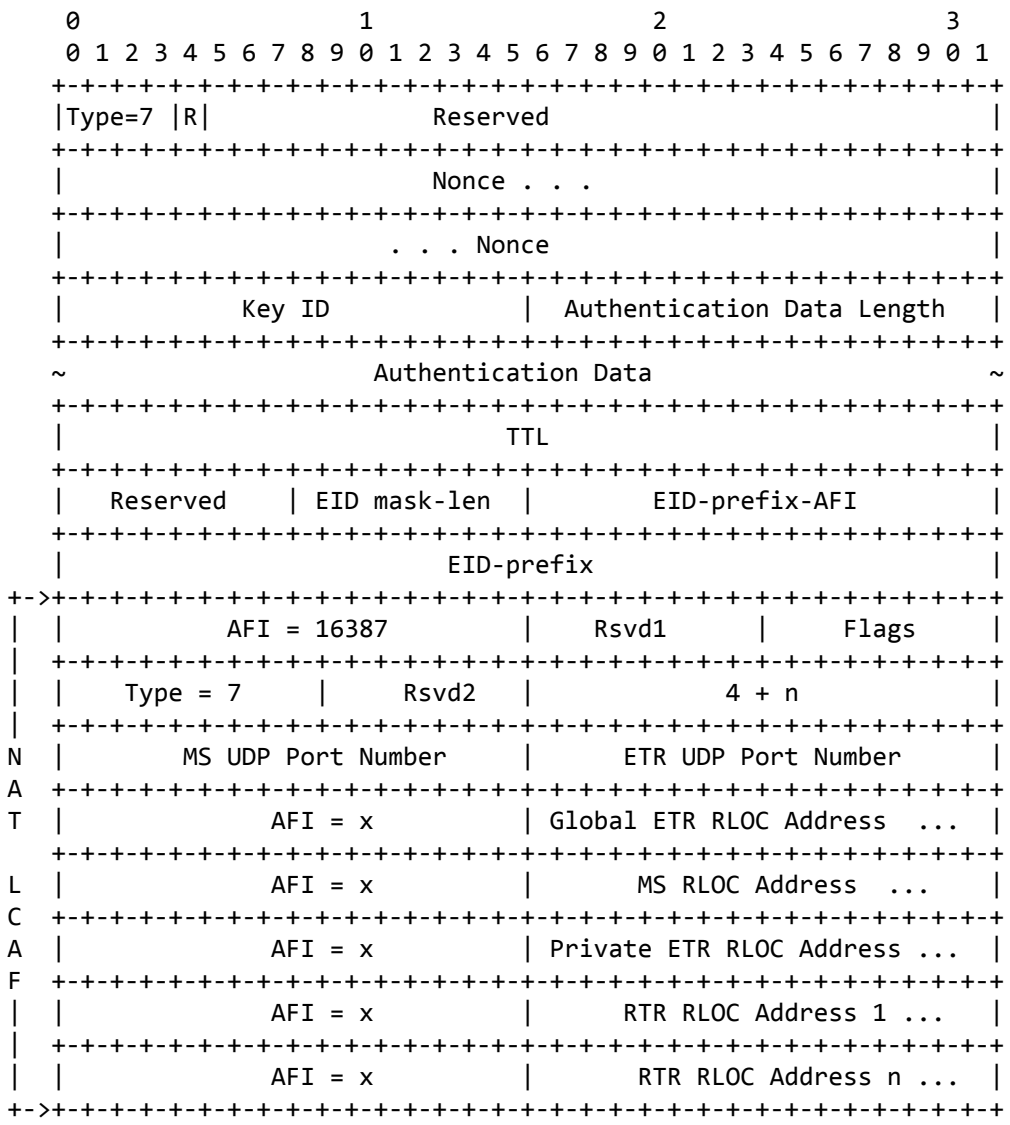
Data Flow II


MS DB:
site1-EID-prefix => RTR-RLOC
NAT State:
ITR-local, 4341 => addr', p'
ITR-local, xxxx => addr'', p''
MS
NAT
Internet
xTR
xTR
LISP DATA
Map-Req/Map-Rep
LISP DATA
RTR
xTR Map-Cache:
0/0 => RTR-RLOC
RTR Cache:
site1-EID-prefix => addr', p' -> RTR-RLOC,4342, ITR-local

Message Formats: Info-Request

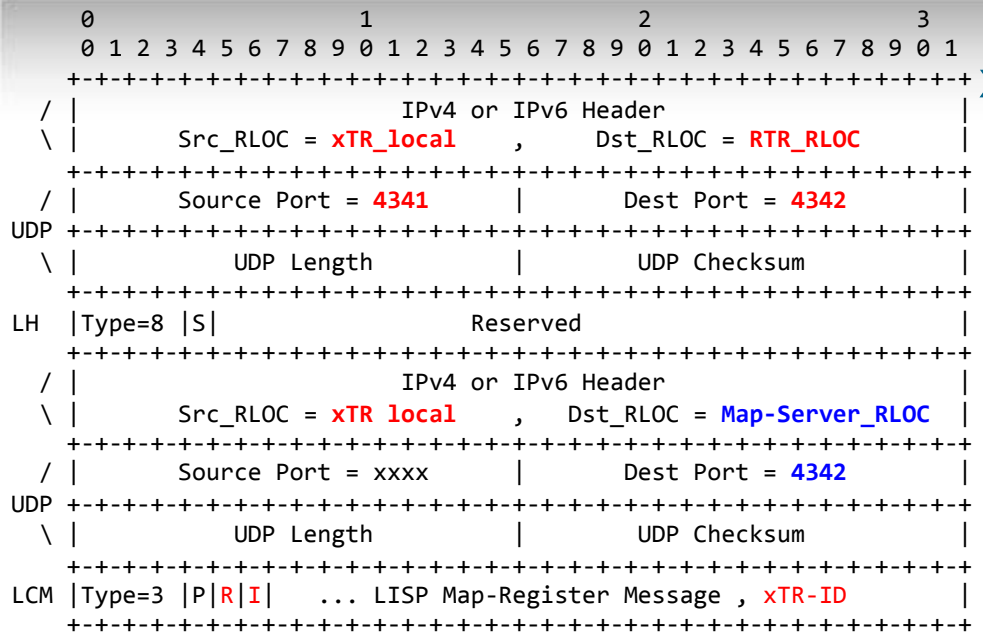


Message Formats: Info-Reply



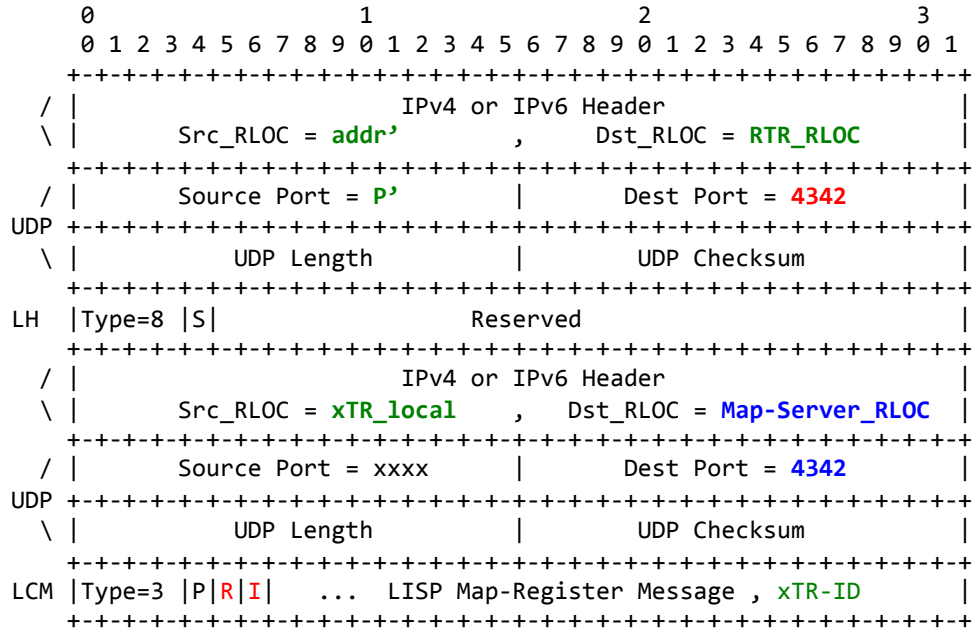
Map-Register (xTR->RTR->MS)

xTR/MN

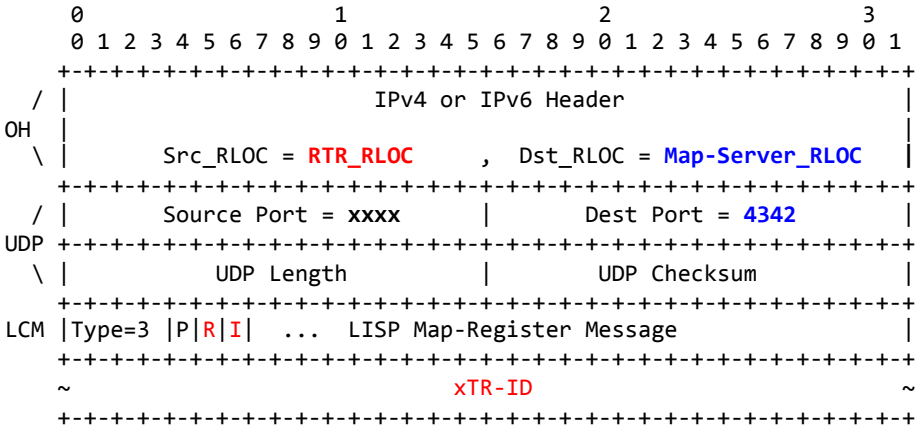


NAT

RTR

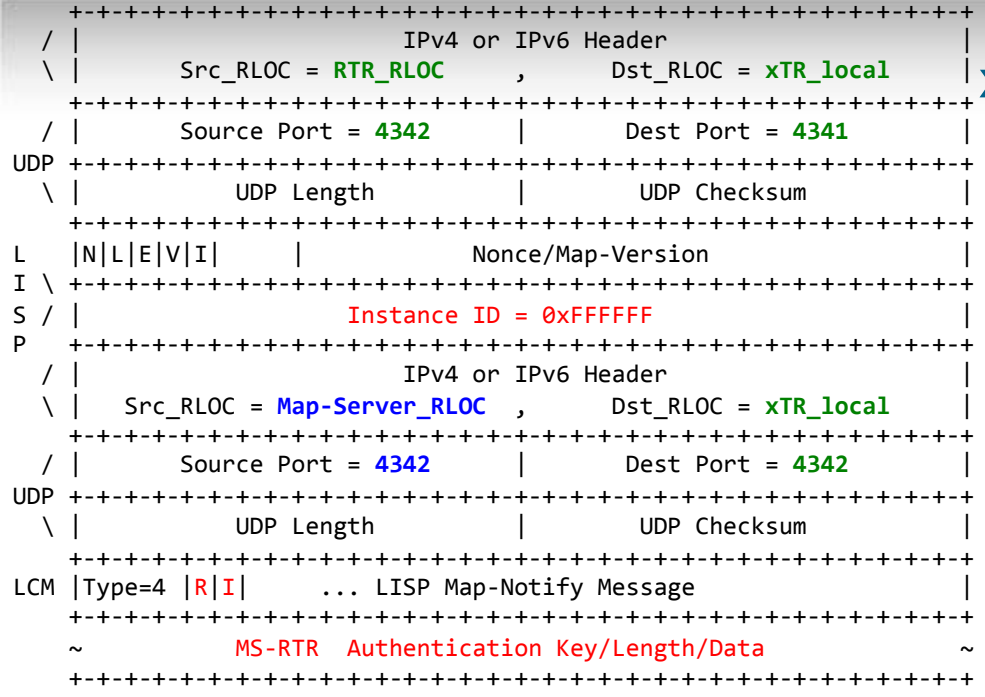


MS



Legend:
Green: Fields to be cached by RTR
Red : Fields that are new,
or are important to NAT Traveral

Map-Notify (xTR<-RTR<-MS)

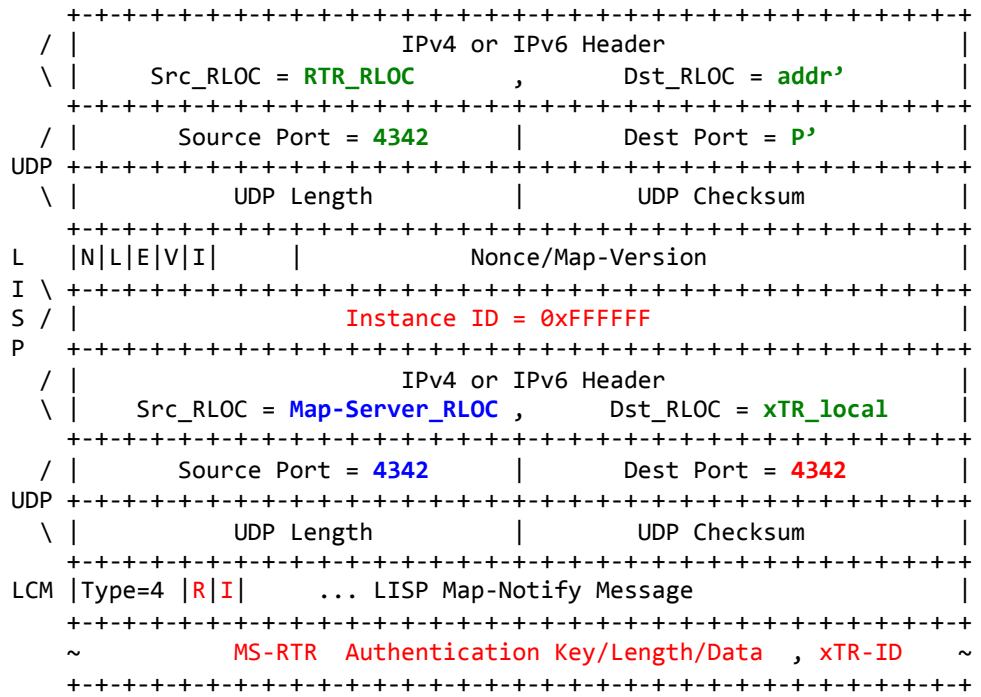


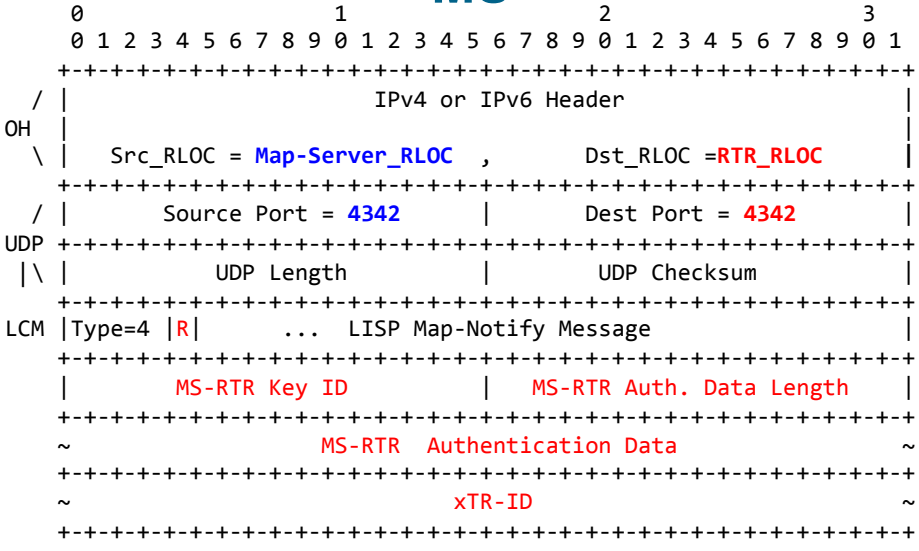
xTR/MN

NAT

RTR

MS



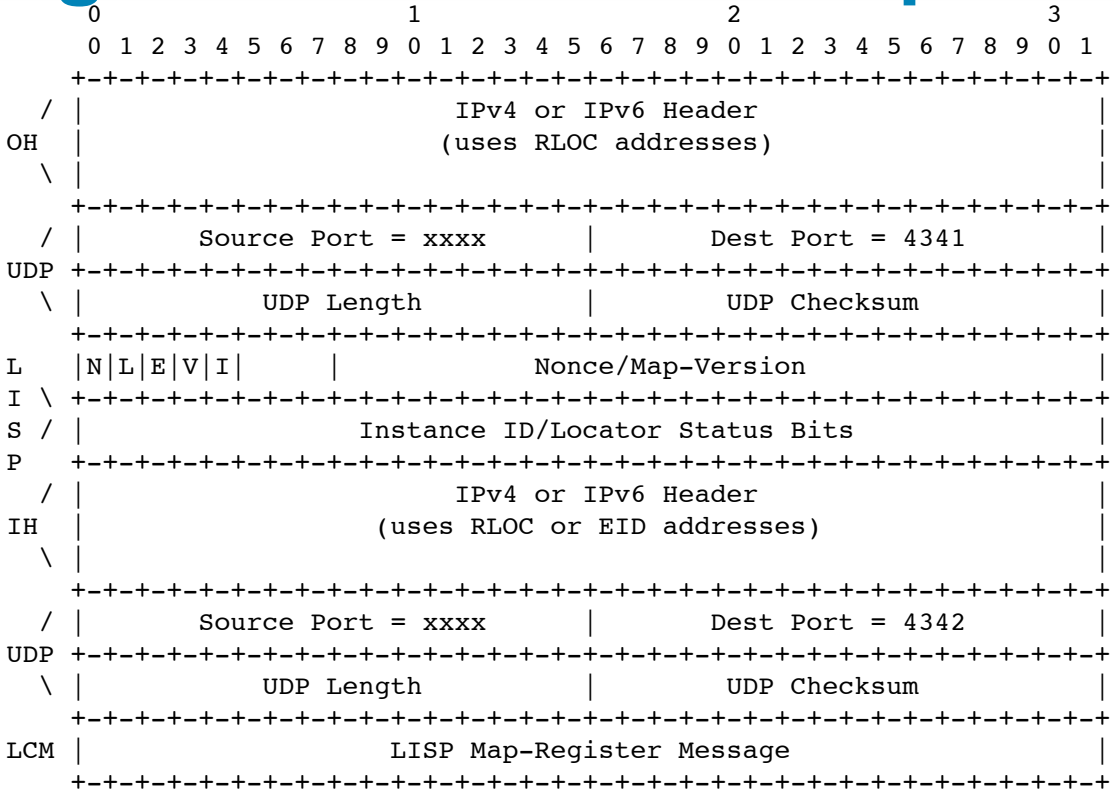


Legend:
Green: fields that are fetched from RTR cache
Red : fields that are new,
or are important to NAT Traversal

Q&A?

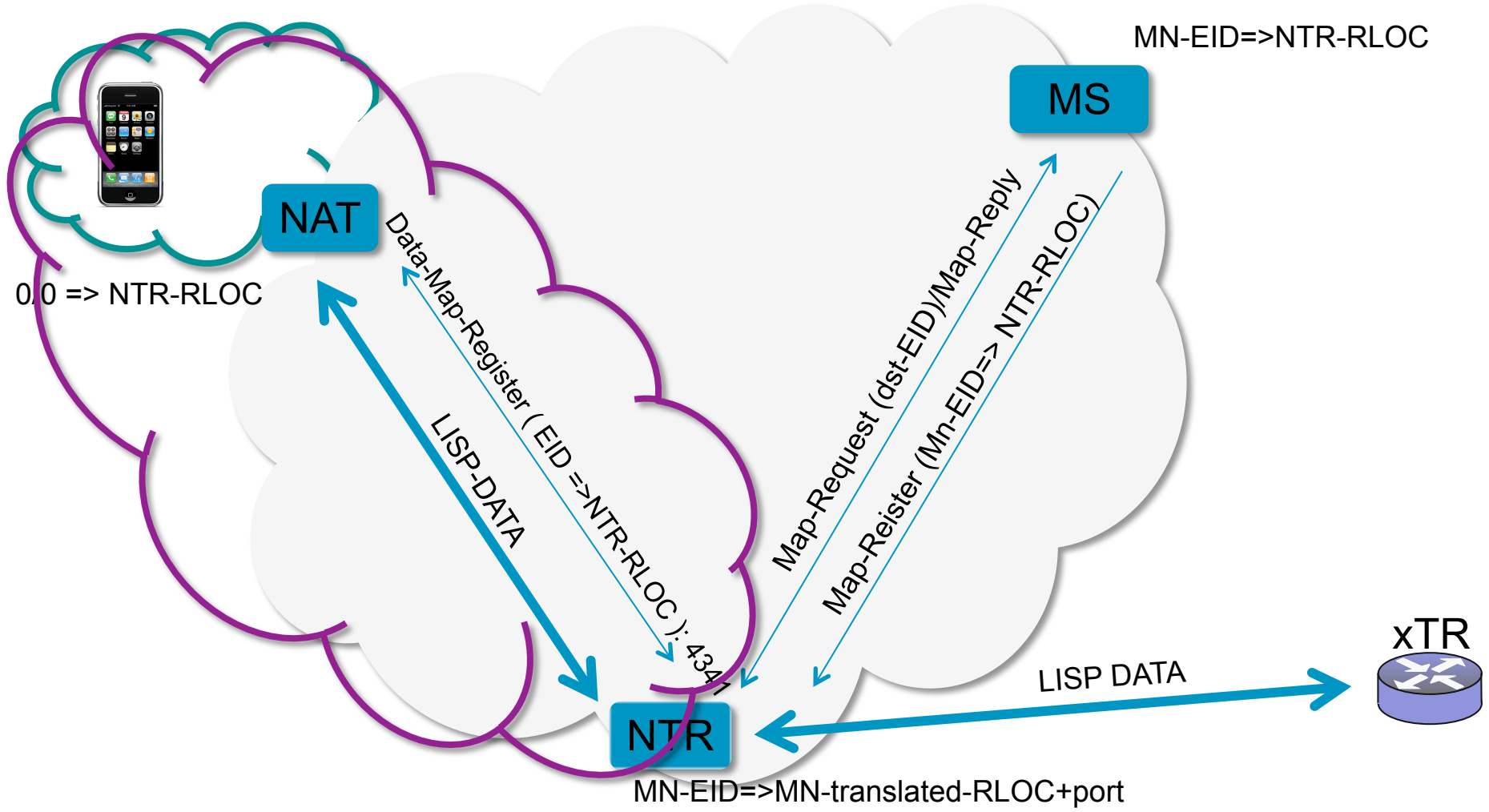
- Thank you!

Message Formats: Data-Map-Notify



- NTR infers MN **translated RLOC and port** from the outer header of this message. This address is cached by NTR and is used by NTR to send data to MN.
- Basically Data-Map-Register functions as an **authenticated Echo Request** message.
- Router Alert is used on LISP data packets that include LISP control payload, so NTR knows that it has to process them differently.
- Inner header destination RLOC must be set to MN's Map-Server RLOC. NTR retrieves this RLOC to identify the MS to send the Map-Register to.
- Inner Header source address should be ignored. NTR re-originates the inner header src addr.

Basic Overview – NTR as re-encapsulating xTR



Essentially, NTR becomes a second xTR for MN. NTR hides MN's mobility events from its corresponding nodes, further ensuring scalability of LISP-MN.