Thin-ICE:
IoT NAT Traversal

Christer Holmberg, Jaime Jimenez, Ari Keränen

christer.Holmberg@ericsson.com
jaime.jimenez@ericsson.com
ari.keranen@ericsson.com

ICE WHAT?

- **I**nternet **C**onnectivity **E**stablishment
- RFC 5245 (2016)
- draft-ietf-ice-rfc5245bis (estimated RFC publication 2017~~7~~8)
- Uses the STUN (Session Traversal Utilities for NAT) protocol for candidate gathering, connectivity checks and keep-alives
- RFC 5245 uses the SDP (Session Description Protocol) Offer/Answer mechanism for candidate exchange
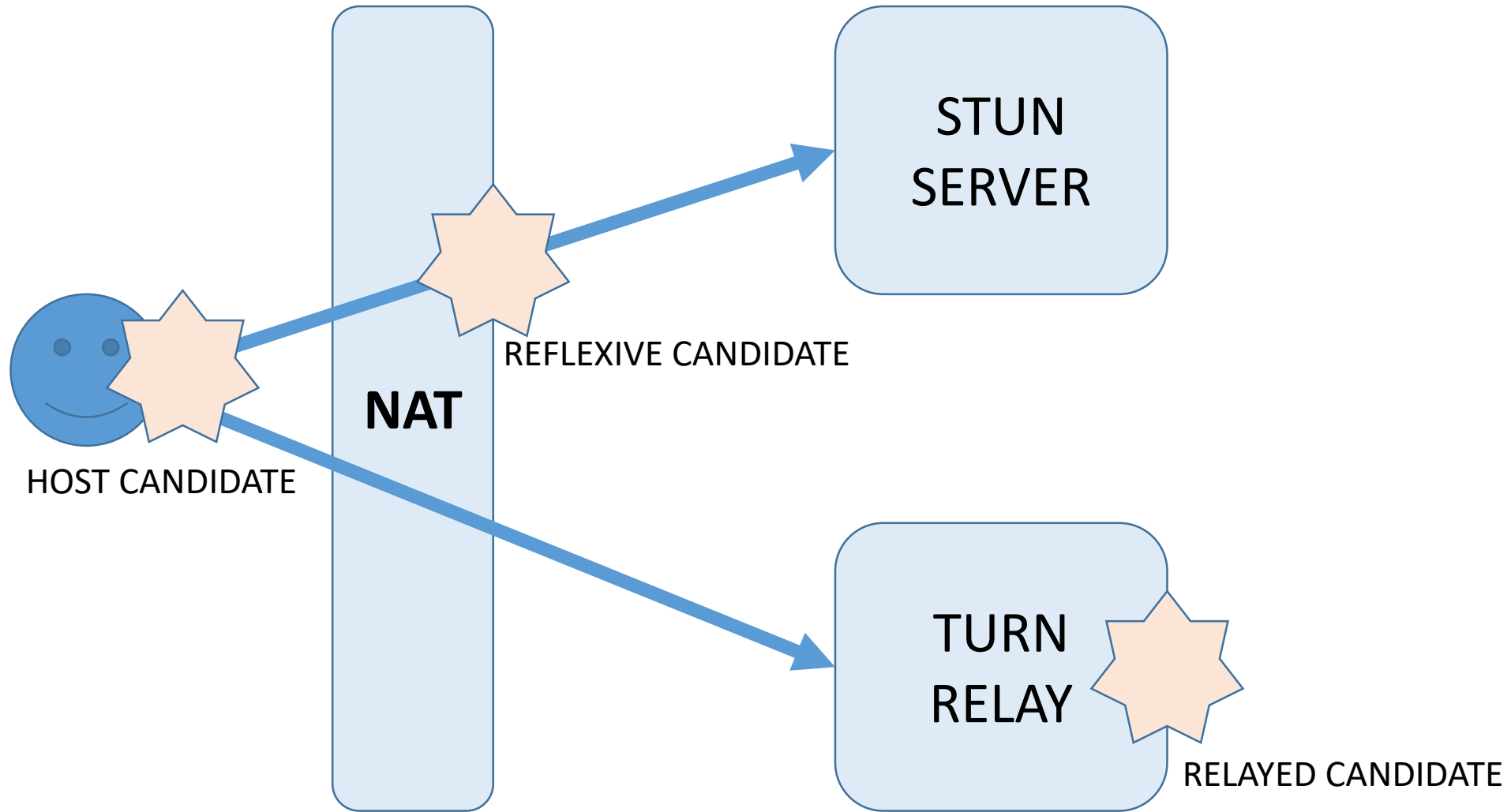- In draft-ietf-ice-rfc5245bis the candidate change protocol is outside the scope

ICE HOW?

- 1. Gather candidates
  - A candidate is a public IP address:port
  - Different candidate types
    - Reflexive: Public IP address:port of port of a NAT
    - Relayed: Public IP address:port of a releay
    - Host: Local IP address:port of endpoint
- 2. Exchange candidates
  - Protocol/mechanism for exchanging candidates outside the scope of ICE core spec
- 3. Test candidates
  - "Connectivity tests"
  - Local candidates form **candidate pairs** with candidates of remote peers
  - Test whether remote peer can be reached using the candidates it provided
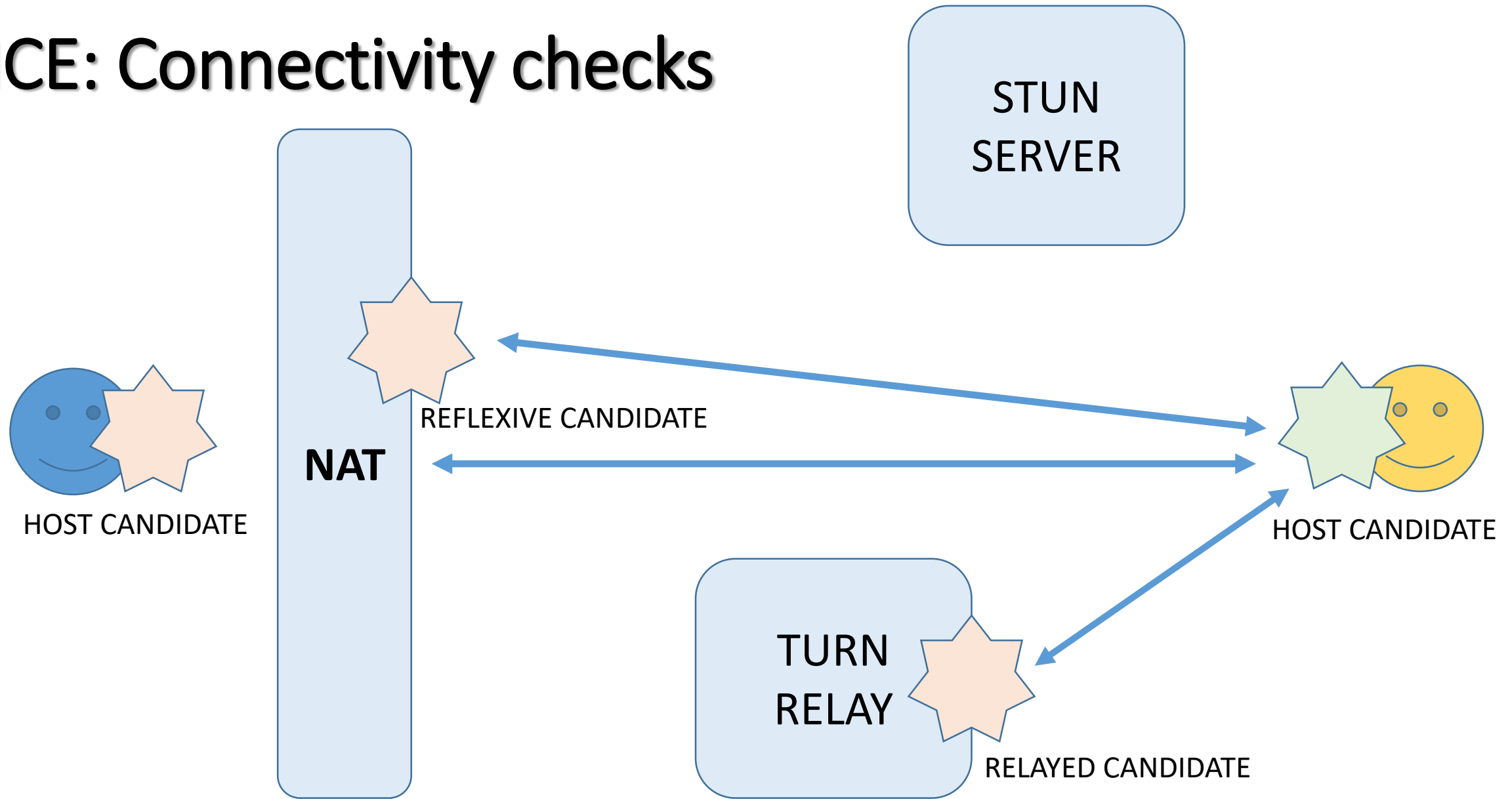 - STUN protocol

ICE HOW?

- 4. Nominate candidate pair
  - One of the endpoints chooses a candidate pair to be nominated
  - Informs the remote peer about the nominated pair
  - The IP addresses:ports associated with the pair will be used
- 5. Keep-alives
  - Periodic keep-alives in order to keep NAT bindings open

ICE: Gather candidates

ICE: Connectivity checks

STUN
SERVER

REFLEXIVE CANDIDATE

NAT

HOST CANDIDATE

HOST CANDIDATE

TURN
RELAY

RELAYED CANDIDATE

Thin-ICE: NUTSHELL

- Use legacy ICE as base
- Only define Thin-ICE specific deltas
    - CoAP protocol instead of STUN
- "T-STUN": function to return public IP address of entity
- Possibility to use existing CoAP intrastructure instead of STUN servers
    - Resource Directory (RD)
    - CoAP broker
- Mechanism(s) for peers to exchange candidate information

Thin-ICE: "T-STUN"

- **WHAT?**
  - CoRE resource
  - Returns NAT public IP address:port to entity behind NAT
  - Will be used to generate reflexive candidate
- **FIND?**
  - Can be requested from a CoRE Resource Directory (RD)
    - Entity that stores information about resources
    - Provides API for registering and lookup of resources
  - CoRE Web Linking (if server hosting T-STUN is known)
- **WHERE?**
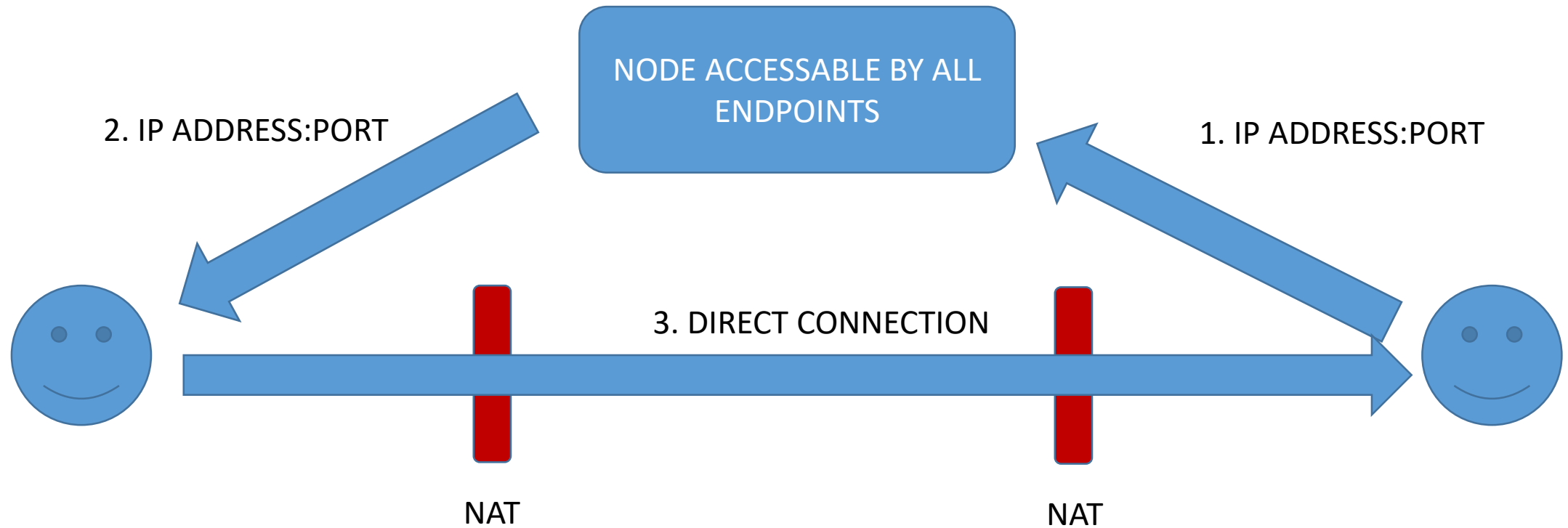 - Can be stand alone node or co-located with other nodes

Thin-ICE: NOTE THIS

- Support not required by the NAT

- Keep-alives required in order to maintain NAT binding

- No new protocol needed

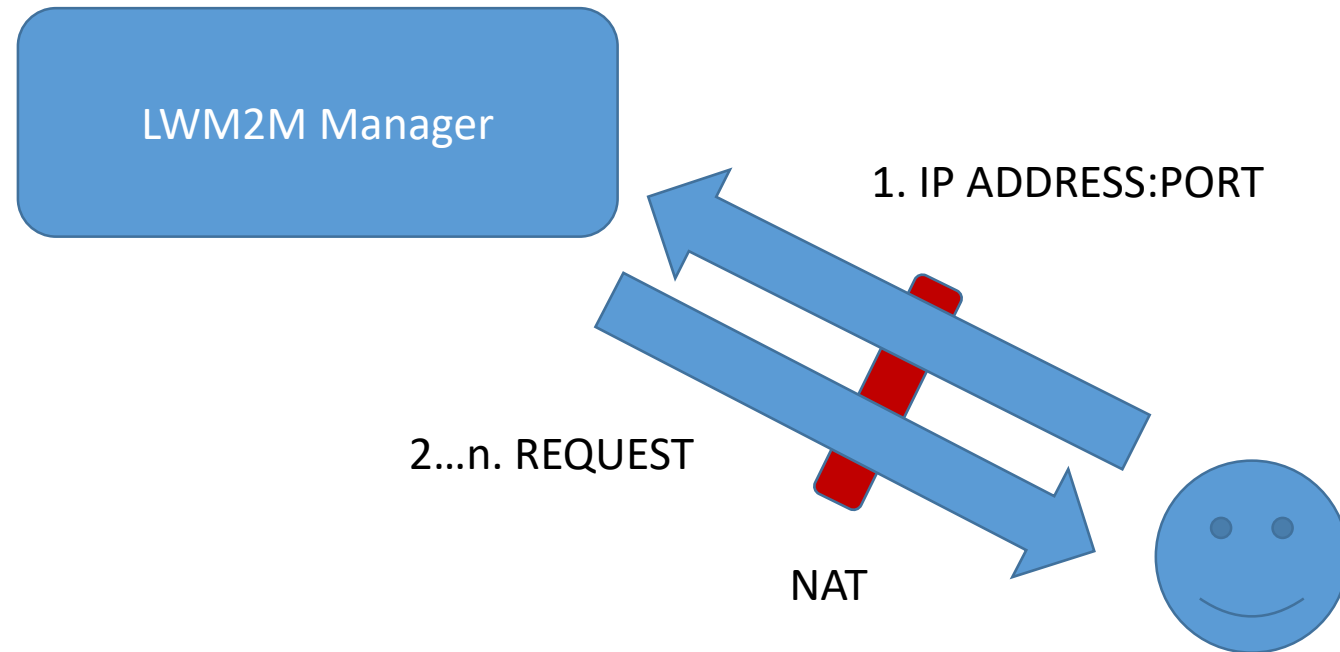- Additional functionality: T-STUN server for returning reflexive address

IP ADDRESS:PORT EXCHANGE

- LWM2M Object

- CoAP pubsub
  - Endpoint publishes it's public IP address:port information
  - Remote peer subscribes to IP address:port information

IP ADDRESS:PORT EXCHANGE: LWM2M

LWM2M Manager

1. IP ADDRESS:PORT

2...n. REQUEST

NAT

THANK YOU!