IoT NAT Traversal

Christer Holmberg

christer.Holmberg@ericsson.com

AGENDA

- Thin-ICE: ICE for IoT
- PCP for IoT

ICE WHAT?

- **I**nternet **C**onnectivity **E**stablishment
- RFC 5245 (2016)
- draft-ietf-mmusic-rfc5245bis (estimated RFC publication 2017)
- Uses the STUN (Session Traversal Utilities for NAT) protocol for candidate gathering, connectivity checks and keep-alives
- RFC 5234 the SDP (Session Description Protocol) Offer/Answer mechanism for candidate exchange
- In draft-ietf-mmusic-rfc5245bis the candidate change protocol is outside the scope

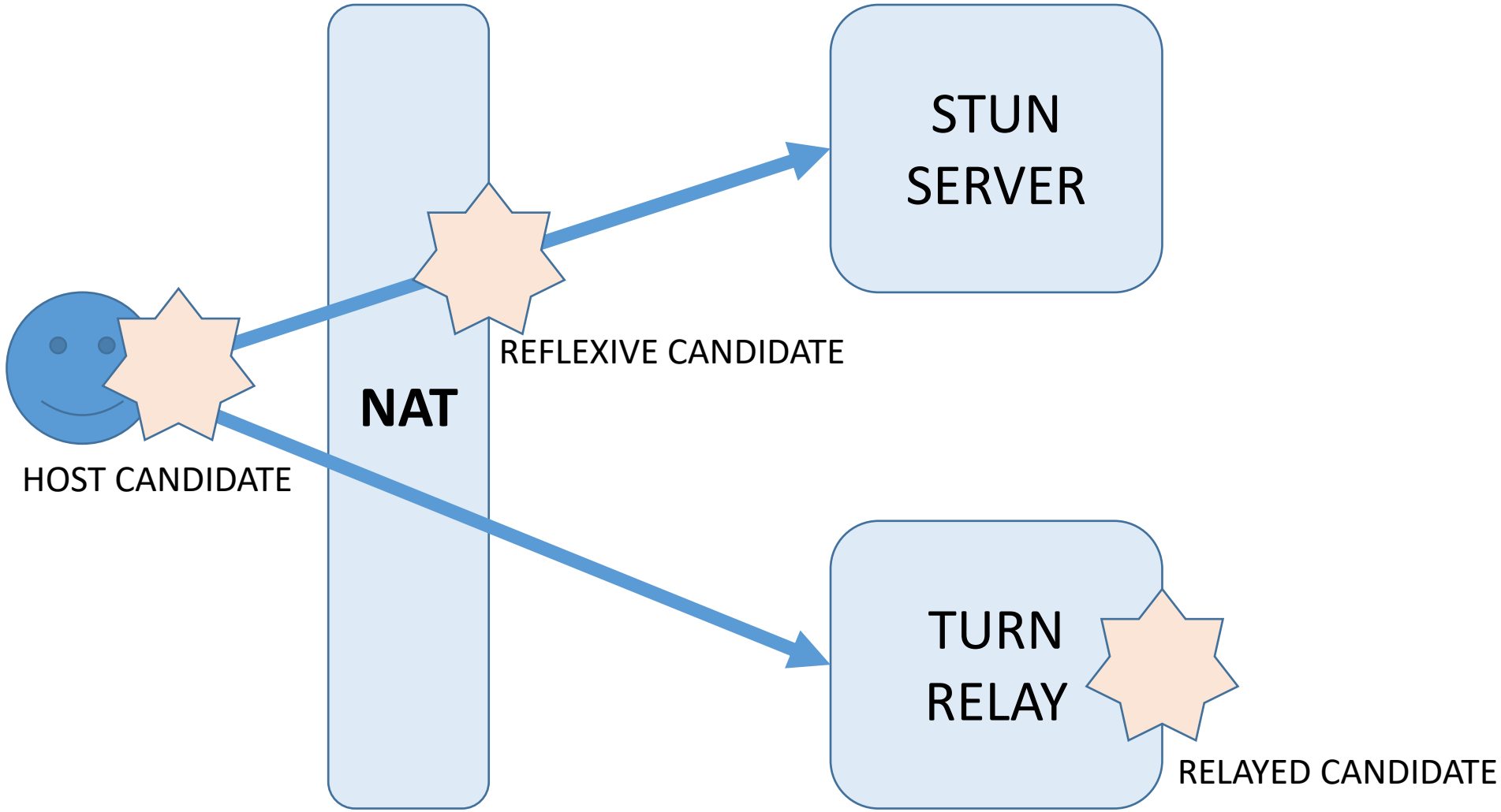
ICE HOW?

- 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

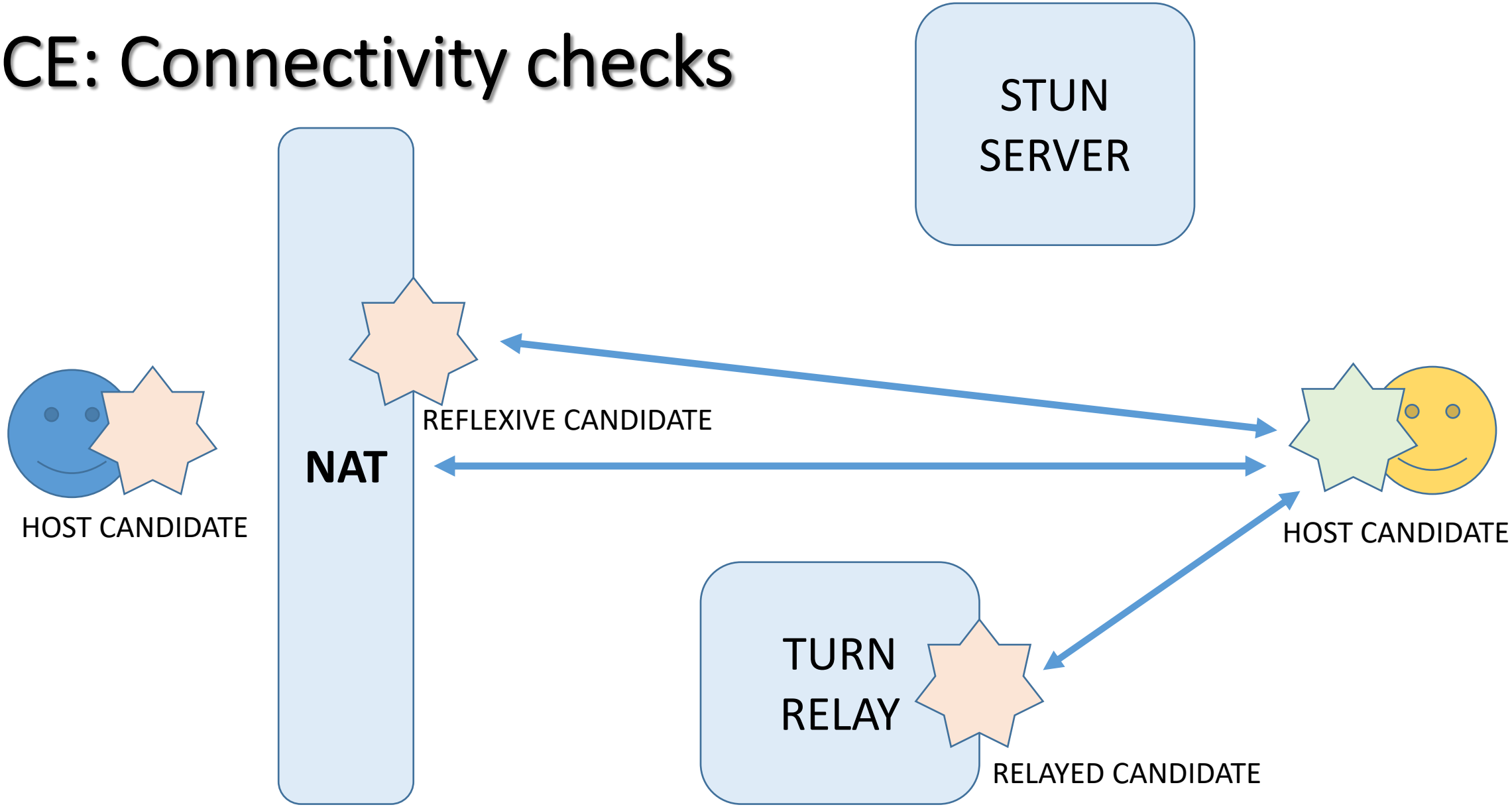
ICE HOW?

- 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



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

PCP (Port Control Protocol): NUTSHELL

- IETF RFC 6887
- Allows an endpoint to control how incoming packets are translated and forwarded by a Network Address Translator (NAT) or simple firewall.
- Create mappings from an external IP address and port to an internal IP address and port.
  - Long time (e.g., web camera) or short time (e.g., on-line game)
- After a mapping is created, remote peer must be informed about the IP address and port for the incoming connection.
  - Application-specific manner

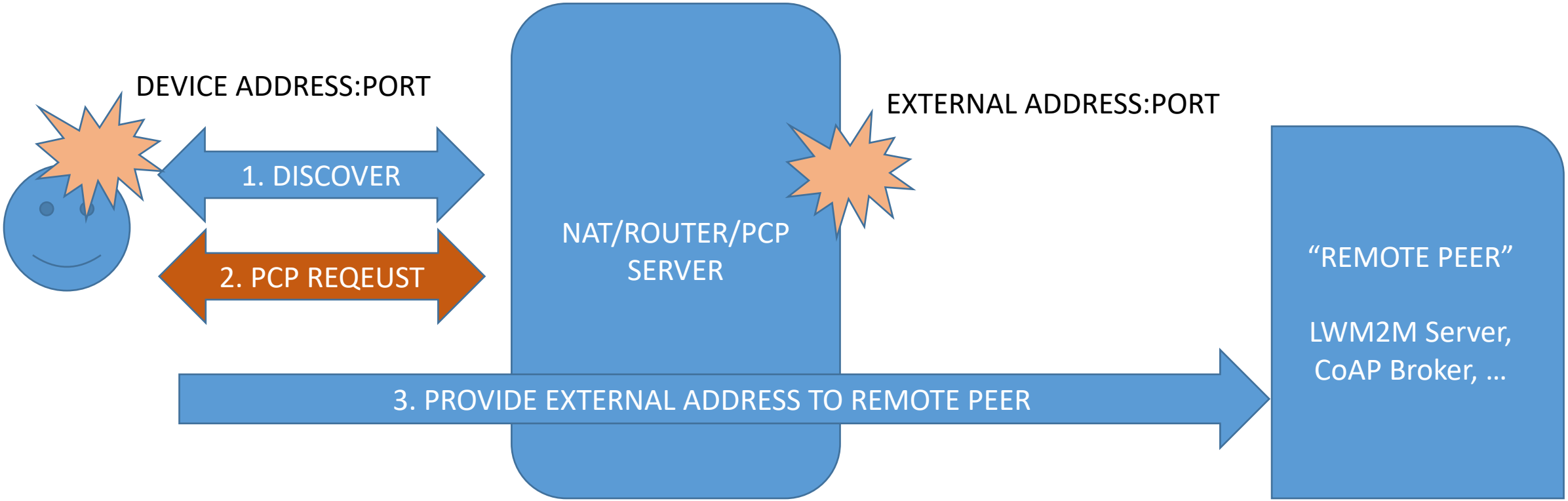
PCP: PROTOCOL DETAILS

- UDP
- Request/Response
- Maximum UDP payload length of 1100 octets.
- PCP messages contain a request or response header containing an Opcode, any relevant Opcode-specific information, and zero or more options.
  - Opcode: A 7-bit value specifying the operation to be performed.
    - Opcode-specific payload
  - Requested lifetime
- Request action for specific local port, or all ports
- PCP response contains assigned IP address:port
- PCP server discovery
  - Configuration (file, DHCP,…)
  - Default router list

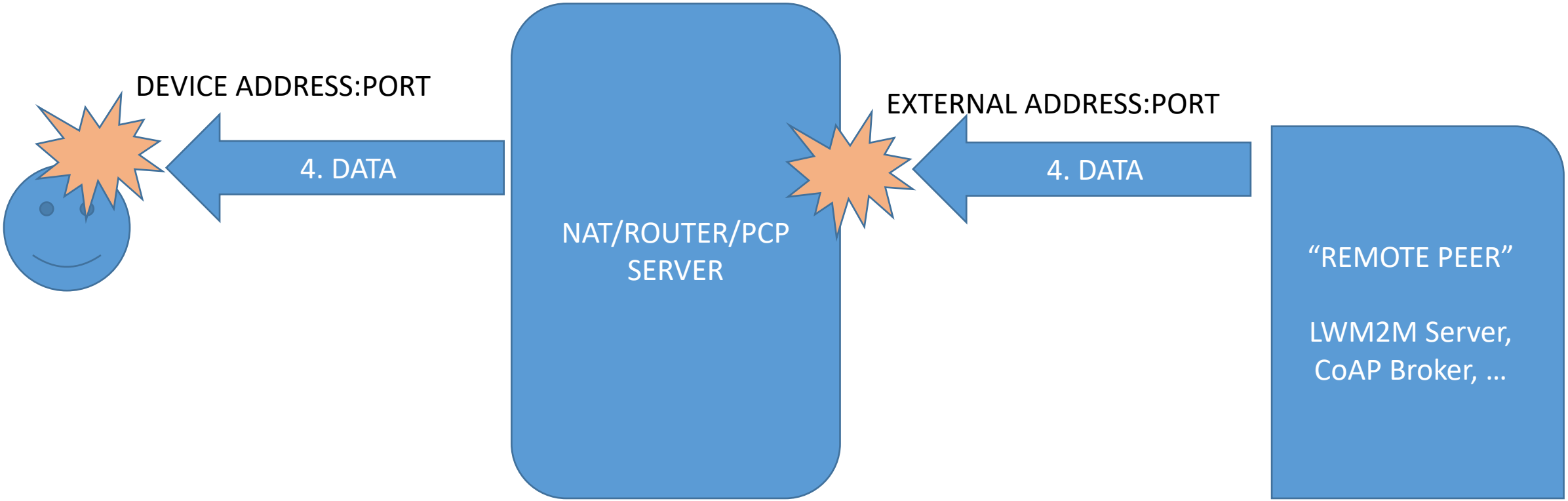
PCP (Port Control Protocol): NOTE THIS

- Support of PCP required by the NAT/firewall
- Keep-alives not requires in order to maintain NAT binding
- No need for additional infrastructure
- Can be used with firewalls
- Only UDP required
- IMPACT ON REMOTE PEER:
  - Needs to support the mechanism used by the client for providing the external address to the peer
  - Remote peer does not need to support PCP

PCP: THE FLOW


DEVICE ADDRESS:PORT
1. DISCOVER
2. PCP REQEUST
NAT/ROUTER/PCP SERVER
EXTERNAL ADDRESS:PORT
3. PROVIDE EXTERNAL ADDRESS TO REMOTE PEER
“REMOTE PEER”
LWM2M Server, CoAP Broker, …

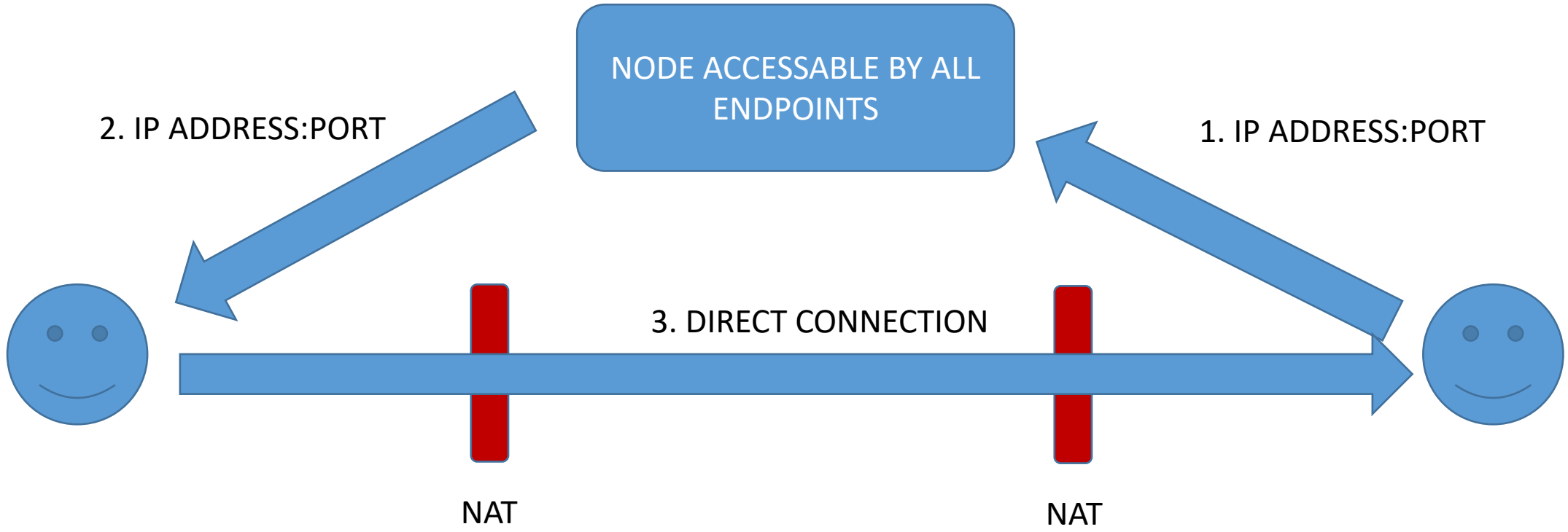
PCP: THE FLOW


DEVICE ADDRESS:PORT
4. DATA
NAT/ROUTER/PCP SERVER
EXTERNAL ADDRESS:PORT
4. DATA
“REMOTE PEER”
LWM2M Server, CoAP Broker, …

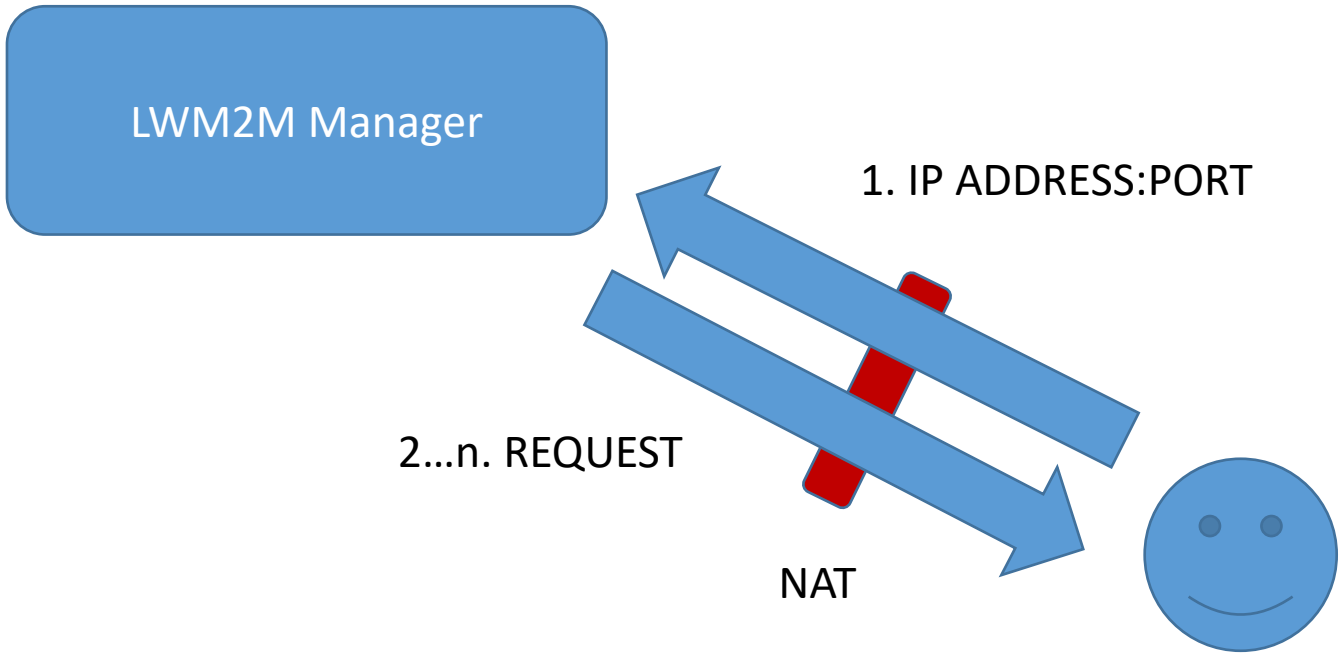
IP ADDRESS:PORT EXCHANGE

- 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: M2M (Direct)



IP ADDRESS:PORT EXCHANGE: LWM2M



THANK YOU!