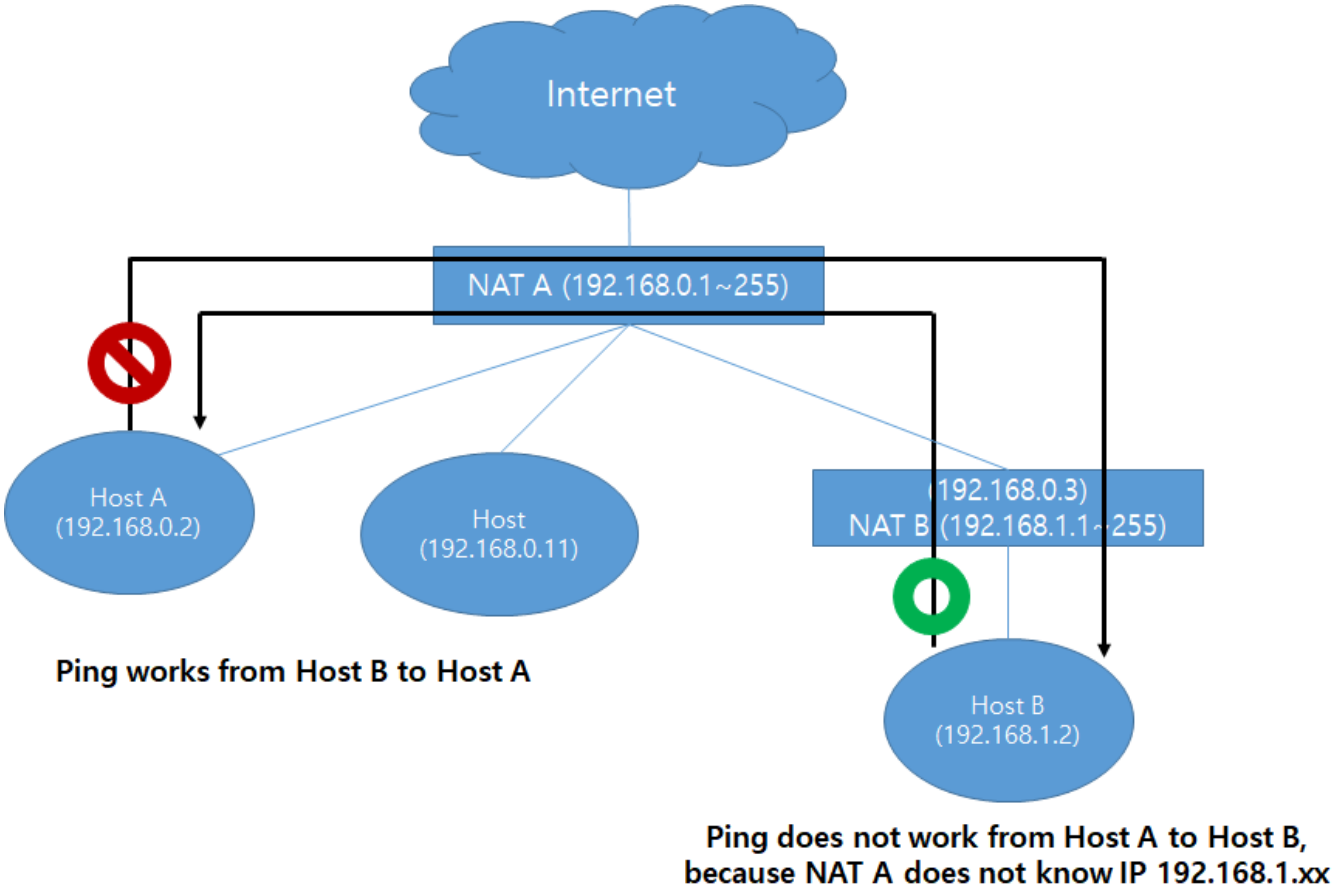
Multi-NAT Communications

Problem statement

When devices are connected under multiple levels of NATs (or routers), the devices under upper levels cannot reach the devices under the lower ones directly even if they know the IP address (Network limitation). With the **Multi-NAT Edge Device Communications (MNEDC)** system, the devices can communicate with each other once they establish a persistent connection with MNEDC server which is running on topmost level of NAT, acting as a relay between devices and helping in communication by providing a channel.



MNEDC Server

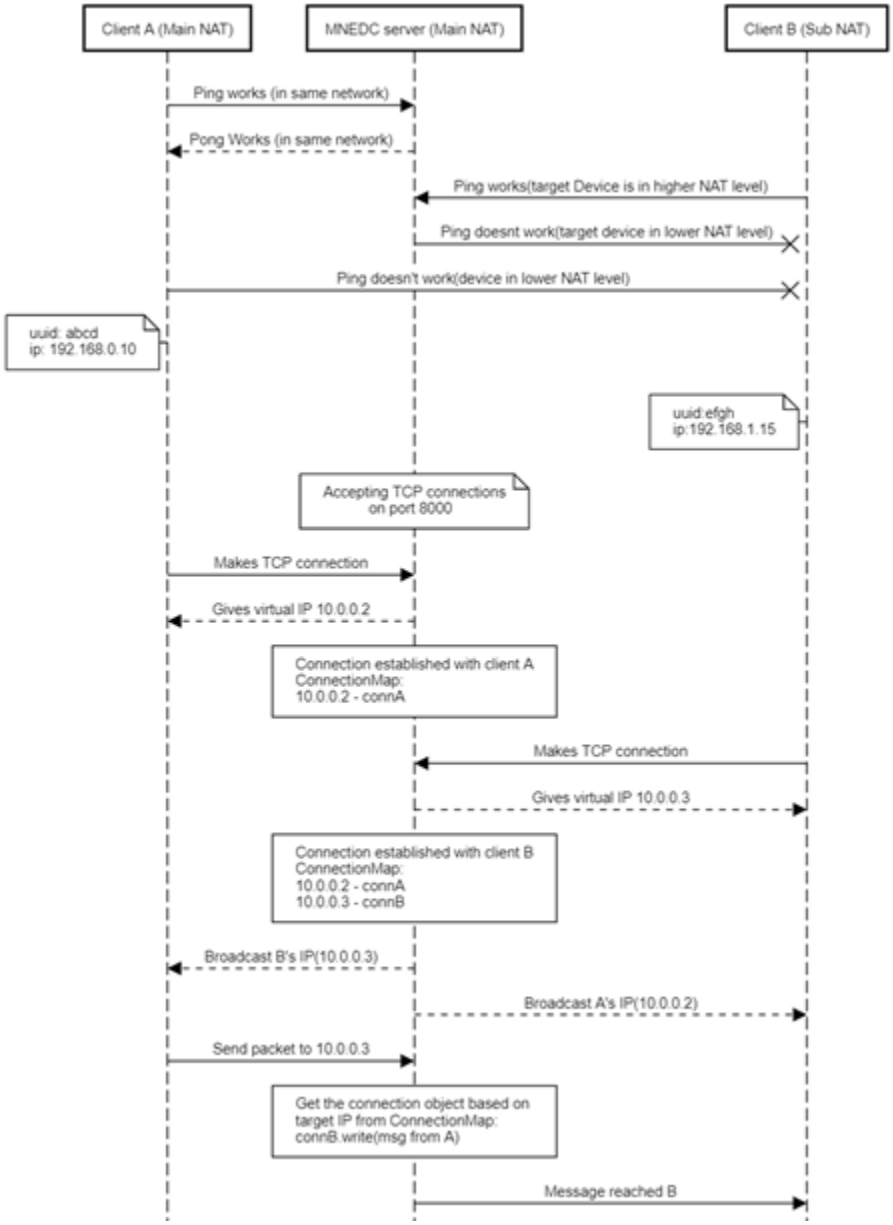
This is a TCP server running on any one of the devices which is reachable from all other IoT devices in the network. Since Sub NAT devices can reach Main NAT device and the other way round is not possible, we need to run the MNEDC server in the Main NAT. This MNEDC Server registers the client whenever the request comes and establishes a persistent connection. Also, it provides it with a unique virtual IP in the address space of 10.0.0.1~255. Then it maintains a key-value map of the unique virtual IP and the TCP connection object. Now the role of server is to get the packets from clients, extract the target virtual IP, and write the packets on the TCP connection object which is retrieved from the map. In this way a device anywhere in the network can communicate with all the devices irrespective of their position in network.

MNEDC Client

The job of the client is to first create a TCP connection with the MNEDC Server and upon receipt of the virtual IP, create a tun interface and assign the IP as given by the MNEDC Server. Then the client reads all the packets on the tun interface and write those packets on the TCP connection established with the server, and capture the packets on the TCP connection and write those on the TUN interface. In this way applications using virtual IP to communicate with the peers will be able to send and receive the packets.

Sequence diagram

The sequence diagram of MNEDC is illustrated as follows.



Device discovery with MNEDC

In the scenario under consideration, multicast discovery of devices won't work. We need to take care of it in some other way. In our solution, MNEDC server takes care of device discovery. It notifies already registered devices about the virtual IP of the new device which comes and joins the MNEDC server. The devices then exchange Orchestration Information, once the reachable IP of their peer is received.

Limitations and assumptions

- The MNEDC server should be run inside a device under the Main NAT.
- The IP address of the MNEDC server should be manually entered in all devices in a config file.
- When the current MNEDC server goes down, the communication wont be possible between devices until it comes back online.
- There should be only one Main router in the network and other router(s) should be connected under it.
- All devices should have unique device IDs.
- There should not be more than 255 devices at a time in the network.

Any help with the limitations and assumptions would be welcomed.

Code availability

MNEDC can be available from **Coconut release (Oct. 2020)** from https://github.com/lf-edge/edge-home-orchestration-go/. You can get further information from https://github.com/lf-edge/edge-home-orchestration-go/blob/master/doc/mnedc.md.