AUTHONE

Technische Universität München

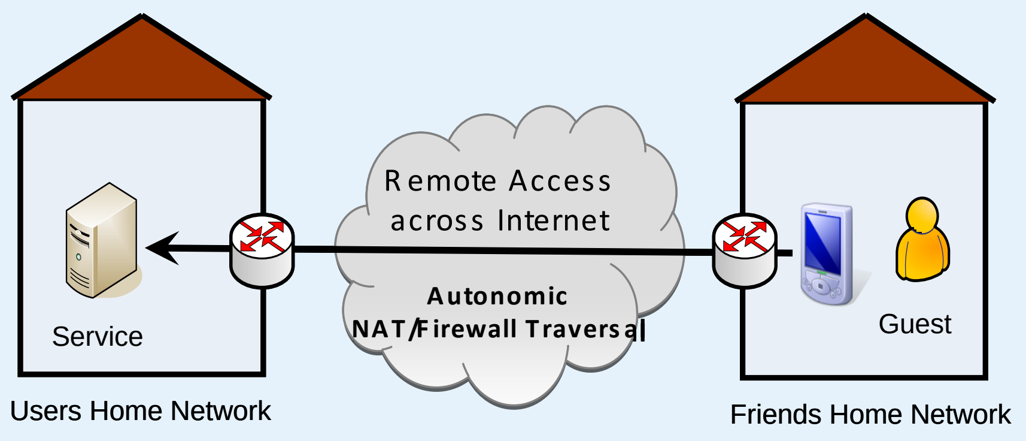
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Andreas Müller
Contact: [mueller]@net.in.tum.de · http://www.net.in.tum.de

Remote Access

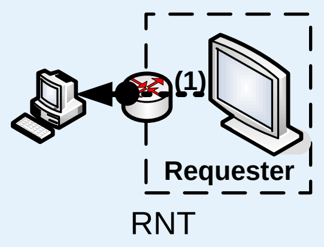
Motivation

- ❑ Easy communication between different networks necessary
  - Access to the video disk recorder
  - P2P applications
  - Facility management applications
- ❑ Most homes use Network Address Translastion (NAT) to access the Internet
  - NAT breaks the end-to-end connectivity model of the Internet
  - NAT/FW-Traversal problem
- ❑ Existing solutions to the problem and their drawbacks
  - Explicit support by the NAT is needed
    - ALG, UPnP, NAT-PMP
  - NAT-behavior based approaches
    - Dependent on knowledge about the NAT
    - Hole-Punching using STUN (IETF - RFC 3489)
  - External Data-Relay (TURN) (IETF - Draft)
    - Routing Overhead
    - Single Point of Failure
  - Frameworks
    - ICE: no TCP, not for legacy applications

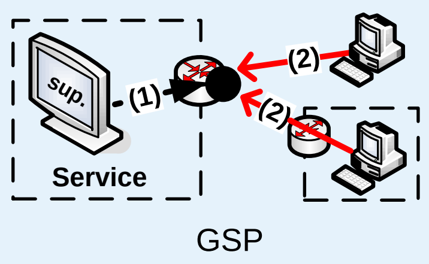


NAT Traversal Service Categories

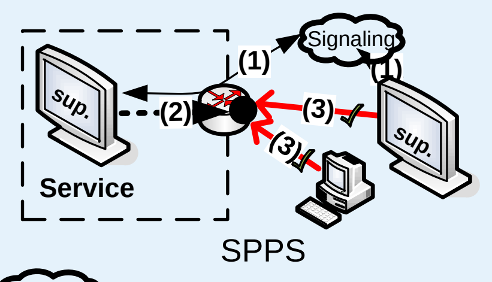
- ❑ Not only the success rate of a NAT-Traversal technique counts
  - Four NAT-Traversal Service Categories were identified for different scenarios
- ❑ Each makes assumptions about the available infrastructure
  - Support at the NAT itself (e.g. an ALG or UPnP)
  - The requester (STUN or signaling)
  - The service (UPnP support at service)
  - The network (presence of infrastructural nodes)



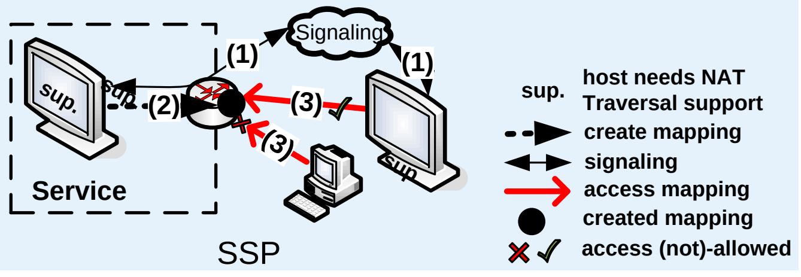
- ❑ Requester side NAT-Traversal (RNT)
  - Applications that actively initiate a connection (e.g. SIP/SDP)



- ❑ Global Service Provisioning (GSP)
  - Service should be globally accessible (e.g. a web server)

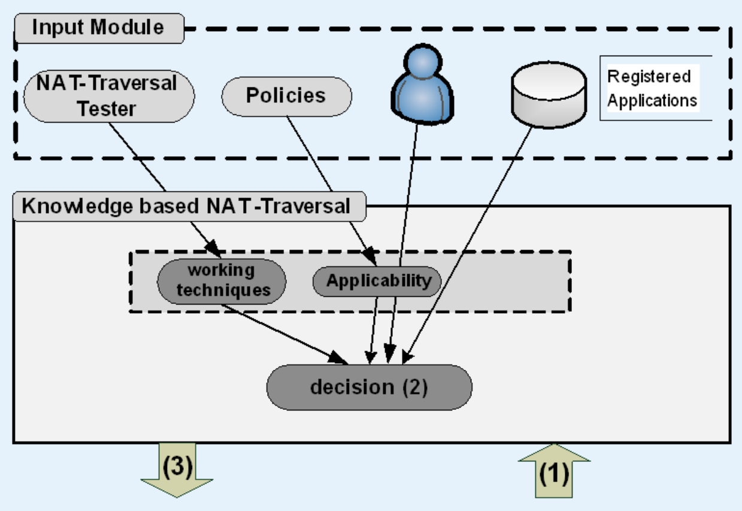


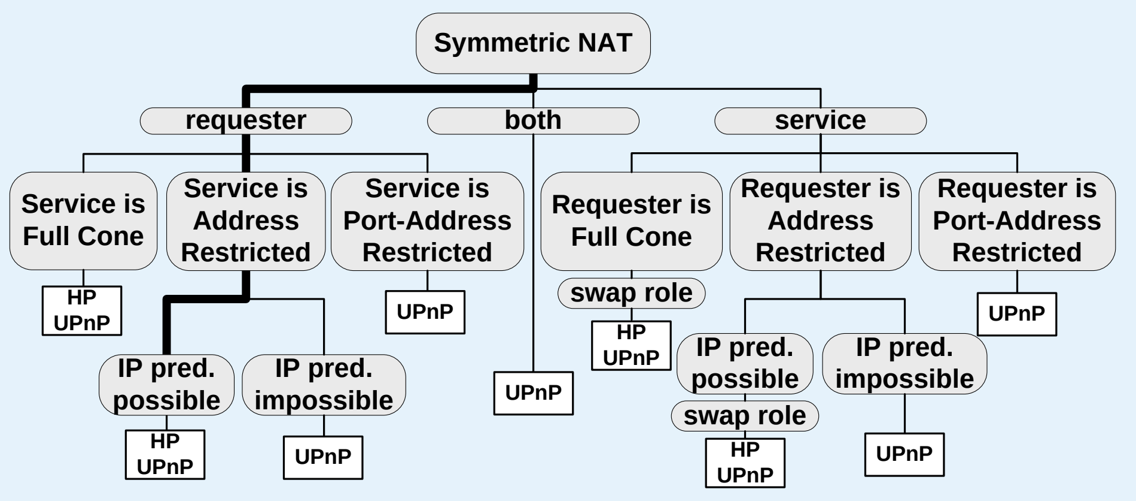
- ❑ Service Provisioning using Pre-Signaling (SPPS)
  - Pre-Signaling through Rendezvous-Point
- ❑ Secure Service Provisioning (SSP)
  - Only authorized users can allocate mappings
  - Created mapping can only be accessed by the creator



ANTS – a knowledge based approach

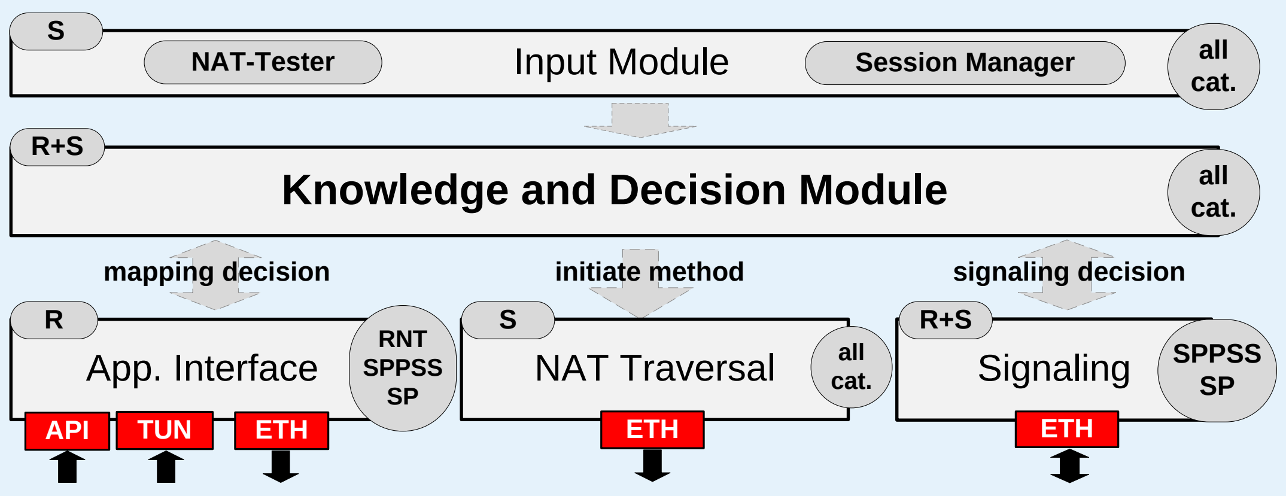
- ❑ The main idea is to create the mapping based on knowledge about the system
  - Which techniques are supported by the NAT
  - What is the NAT constellation
  - Applicability knowledge regarding accessibility of the mapping
    - Which techniques work with the requested Service Category
    - Hole-Punching with GSP only if Full-Cone NAT
    - UPnP not suitable for Secure Service Provisioning
  - User-preferences and policies
    - Switch to UPnP (although unsecure) if nothing else works
    - UPnP may be faster for SSP dependent on the number of consecutive connections



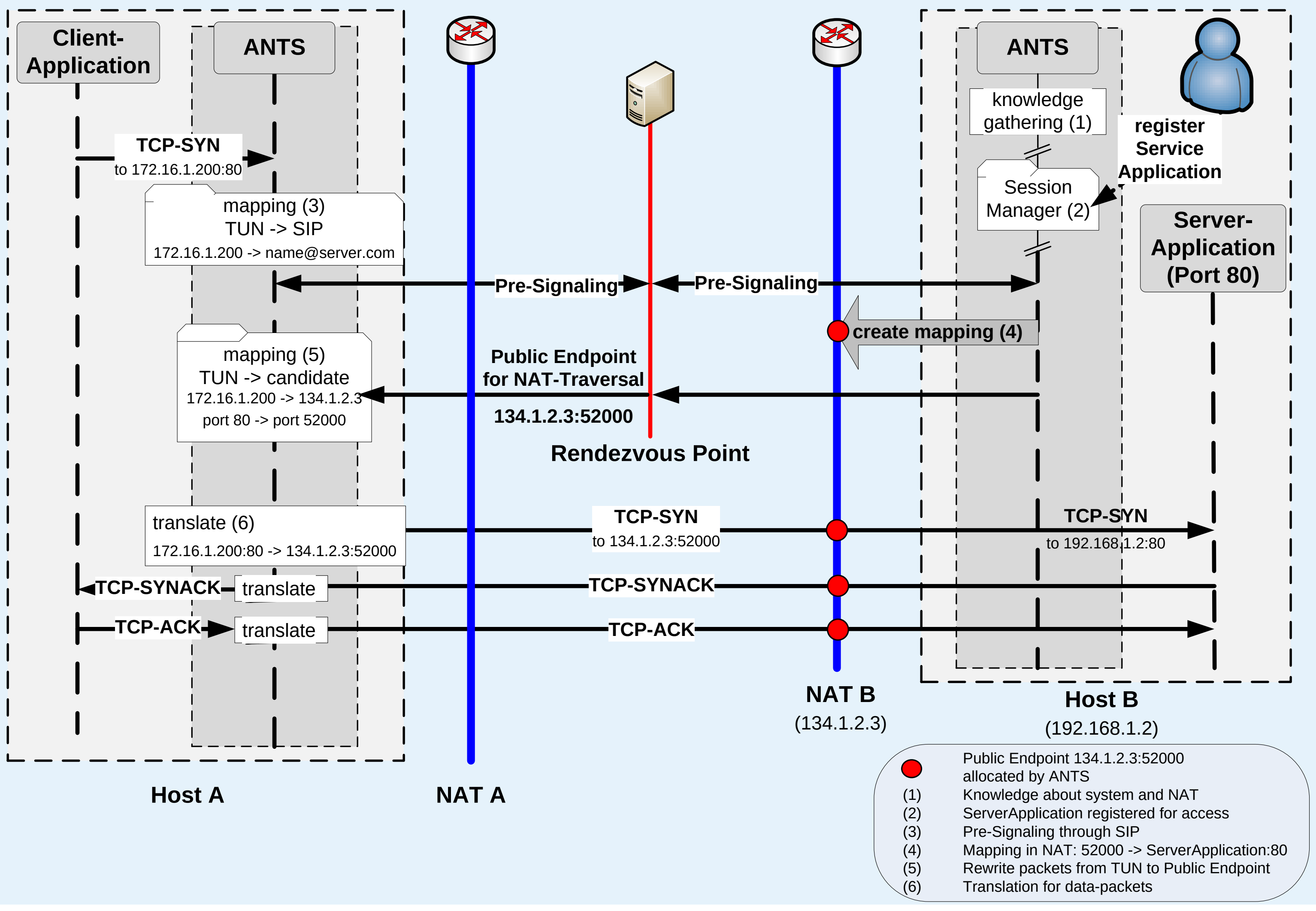


Architecture

- ❑ ANTS architecture consists of three layers and five modules
- ❑ Input Module
  - Session manager holds registered applications
  - NAT-Tester for gathering knowledge
- ❑ Knowledge and Decision Module
  - Makes decisions for the other modules
- ❑ Application Interface
  - ANTS socket API: for new applications
  - TUN-based approach: for legacy applications
- ❑ NAT Traversal Module
  - Actual techniques
- ❑ Signaling Module
  - Parsing of XML-Messages
  - Communication with the RP



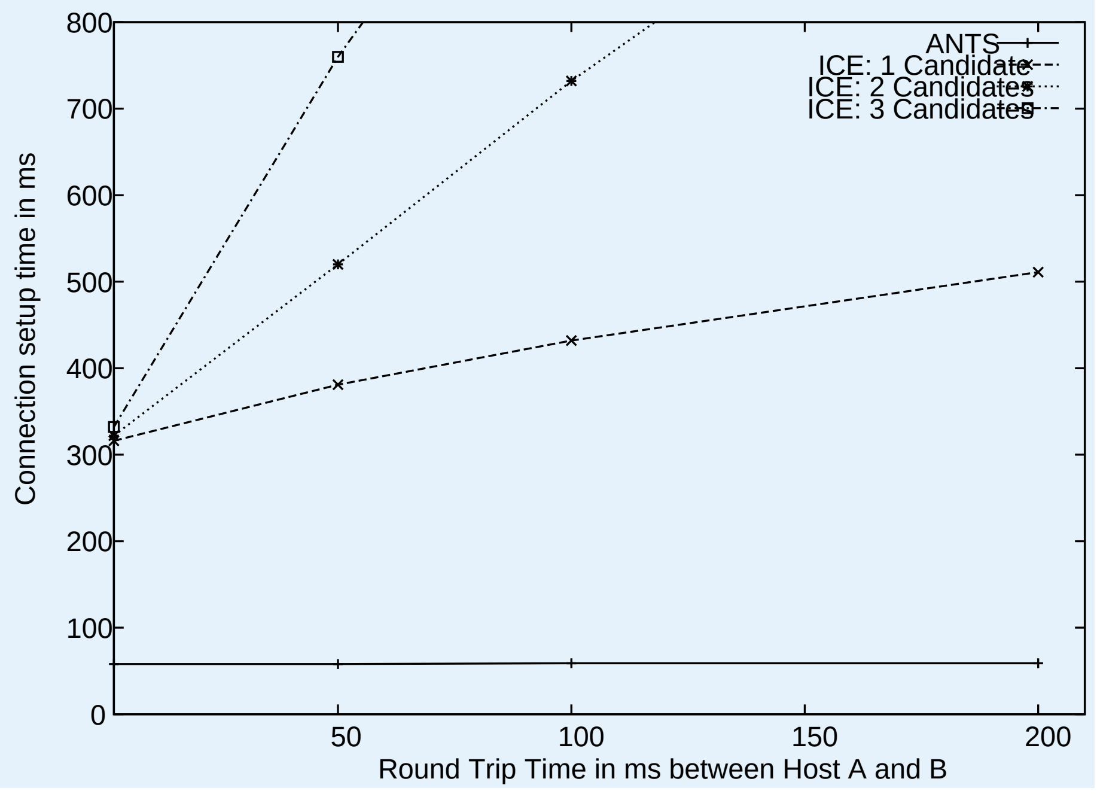
Reference Example for SSP



●	Public Endpoint 134.1.2.3:52000 allocated by ANTS
(1)	Knowledge about system and NAT
(2)	ServerApplication registered for access
(3)	Pre-Signaling through SIP
(4)	Mapping in NAT: 52000 -> ServerApplication:80
(5)	Rewrite packets from TUN to Public Endpoint
(6)	Translation for data-packets

Evaluation

- ❑ Reliability Evaluation
  - Success rates for different NAT-Traversal techniques
  - Results adapted to our defined service categories
  - We did a public field test covering > 1200 different NATs in the wild
  - NAT-Tester and detailed results at http://nattest.net.in.tum.de
- ❑ Propabilities for a direct connection
  - UDP Traversal: 85%
  - TCP Traversal: 82%
  - TCP inclusive tunneling: **95%**
  - Otherwise: Data relay
- ❑ Performance Evaluation
  - ANTS vs. ICE
  - Introduced delay much smaller and constant due to knowledge based approach


Connection setup time in ms
Round Trip Time in ms between Host A and B
ANTS
ICE: 1 Candidate
ICE: 2 Candidates
ICE: 3 Candidates