Supporting NAT and Firewall Peers in End System Multicast

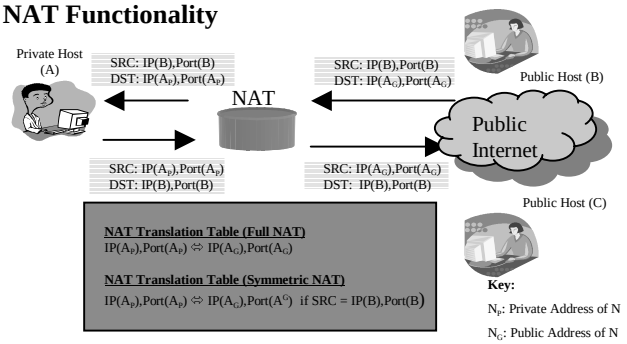
Aditya Ganjam

NAT/Firewall Challenges to Peer-To-Peer

Key Functionality needed by Peer-To-Peer Systems

- Unique Peer Addressing – *A peer must be uniquely addressable by all other peers*
- Bi-directional Connectivity – *Any peer should by able to connect to any other peer*

NAT Functionality



Firewall Functionality

- Allow TCP to initiate connections from within the private network
- Some firewalls block UDP traffic completely

Both NAT and Firewall break key requirements

- IP Addresses are NOT unique
  - Multiple NAT hosts can have the same address
- Ports are NOT well-known
  - Ports can be translated by the NAT
- Unidirectional connection initiation ONLY
  - Only hosts behind NAT or Firewall can initiate the connection
- Source IP Address NOT constant
  - Address for local hosts is Private
  - Address for global hosts is Public
- Translation can timeout

Motivation for Solution for ESM

ESM is an overlay based multicast architecture

- Nodes self-organize by choosing a parent to from the tree
- Overlay tree is optimized for both bandwidth and latency

Why is NAT/Firewall important to ESM?

- Previous broadcast of the SIGCOMM conference showed that almost 25% were behind NAT or Firewall

Why a new NAT/Firewall solution for End System Multicast?

Why not Proxy or Relay solution?

- Protocol depends on peers being able to become parents
- Performs measurements using UDP for optimization

Proposed Solution

Key Features

- Initiate TCP data connection from both parent and child
- Assign unique identifiers and maintain relevant information for each host
- Detect hosts behind same NAT by UDP probing
- Optimize protocol performance by increasing NAT knowledge of public hosts

Strengths

- No infrastructure support needed
- No configuration necessary by the end user

Constraints

- NAT/Firewall hosts cannot communicate with other NAT/Firewall hosts in different networks
- Public hosts can communicate with NAT hosts with some probability (only with Symmetric NAT)

Implications of Constraints

- There exists a threshold of % NAT hosts beyond which a connected tree cannot be constructed assuming bounded degree
- A NAT host has a reduced set of choices for its parent. With Symmetric NAT, a public host has a reduced set of choices for its parent.

Experimentation Results

- Experimented on an Internet test bed with 15 individual machines and 3 virtual hosts on each machine
- Results show that bandwidth degrades with increased % of NAT
  - This can partly be attributed to delayed join with a large % of NAT as can be seen with the 70% NAT run
- The average number of children for public hosts increases and reaches the degree bound of 6 and converges to 1 for NAT (not shown)
- From the resource usage we can see that the optimal delay tree does not degrade too much until very large % of NAT is reached and here it can be very variable
- The tree built by the protocol stays within a constant factor of the optimal even for large % NAT