Host Identity Specific Multicast

Rolland Vida

Budapest University of Technology and Economics

vida@bme.tmit.hu

Presented by Andrei Gurtov

Outline

- Multicast models
- Problems with the current models
- Host Identity Namespace
- Host Identity Specific Multicast model
- Conclusions

Current Multicast Models

- Any Source Multicast (ASM)
  - Oldest model
  - Anyone can join a multicast session
  - Anyone can send to a multicast address
  - Session identified by a multicast group address (G)

- Source Specific Multicast (SSM)
  - Newer model
  - Anyone can join a multicast session
  - Session identified by the source's IP address and a multicast group address - (S, G)
    - Only the source S can send to the group

Problems with the models (I)

- Lack of network level authentication mechanisms
  - There's no control over who can listen to a session
    - If a receiver asks for it, its router will join the tree
    - Multicast Control Protocol (MCOP)
      - Some kind of access control
        - Gives access to subnets, not individual receivers
      - Not used
  - In ASM there's no control over who can be a source
    - In SSM the control is based on the source IP address
      - Easy to cheat – IP address spoofing
  - No appropriate accounting model can be built

Problems with the models (II)

- Hard to handle IP address changes when…
  - Moving into another domain (mobility)
    - Mobile receivers
    - Mobile sources (e.g., video conferencing, online gaming)
  - DHCP assigns a new IP address even if the host (source/receiver) does not move
  - Multi-homed hosts can rapidly change from one interface to another
  - Change from an IPv4 to an IPv6 domain

Handling address changes in multicast

- Receiver side
  - Remote Subscription
    - A new branch of the multicast tree is built
      - In certain cases it might be long
  - Bi-directional Tunneling
    - The original tree is extended with tunnels
    - Triangular routing, inefficient
- Source side
  - No problem in ASM, treated as a new source
  - In SSM, packets accepted only from the original source address
    - The entire tree has to be rebuilt!
    - Time consuming, service interruption

Problems with the models (III)

- IPv4 / IPv6 trees
  - No solution for an IPv4 capable client to subscribe and receive an IPv6 multicast stream
  - Multicast routers can't build dual-stack multicast trees
    - In one session, only one kind of IP identifiers can be used
  - Tunneling through domains with different IP version can be done, but significantly decreases the efficiency

Host Identity Namespace

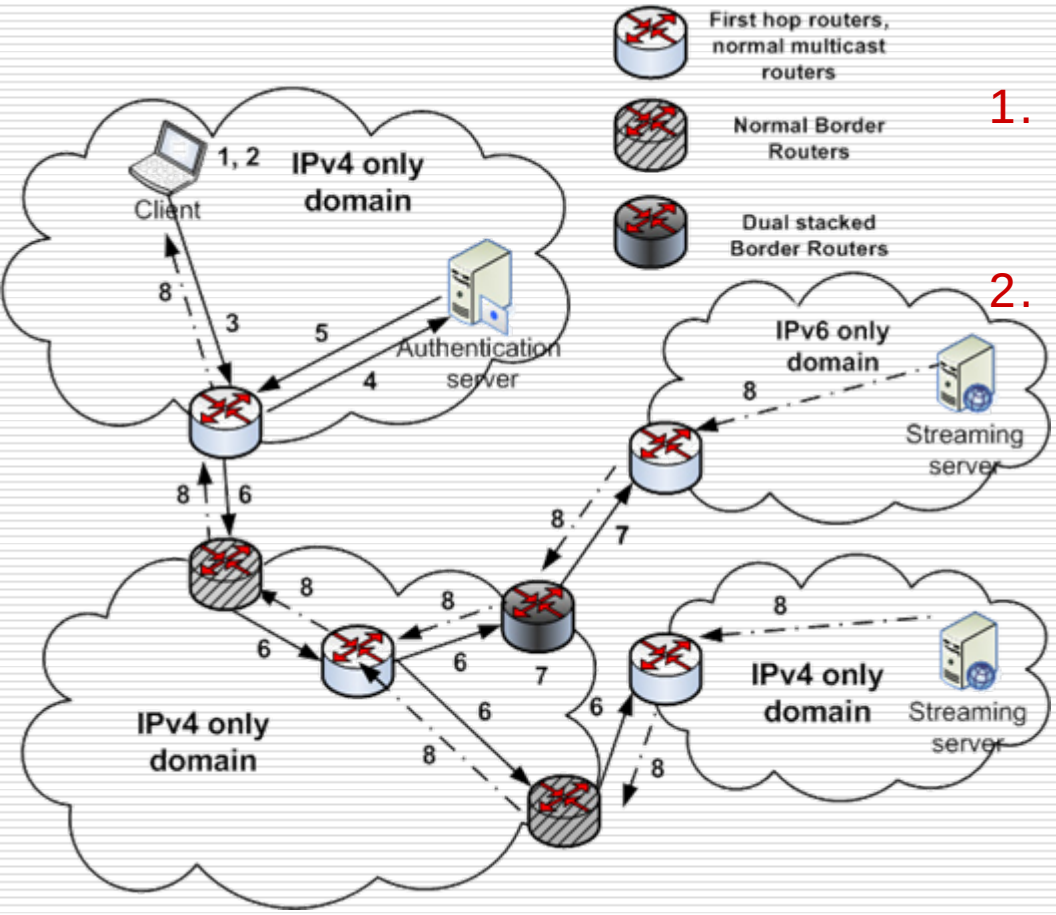
- Some of these problems are due to the dual-role of IP addresses
  - Identifies the host itself
  - Identifies the location / routing functions

- Host Identity Namespace
  - IP address only used for routing
  - Host Identity Tags (HIT)
    - 128 bit long
    - Hashed from the Host Identity
    - Cryptographic identities, public keys

Host Identity Specific Multicast

- Identifiers
  - Source address (S) -> Source HIT (HIT-S)
    - HIT-S never changes
  - Group address (G) -> Session ID (SID)
    - SID independent from the IP version of the multicast stream, 26 bit long
  - HIT-R – HIT of the Receiver

Host Identity Specific Multicast

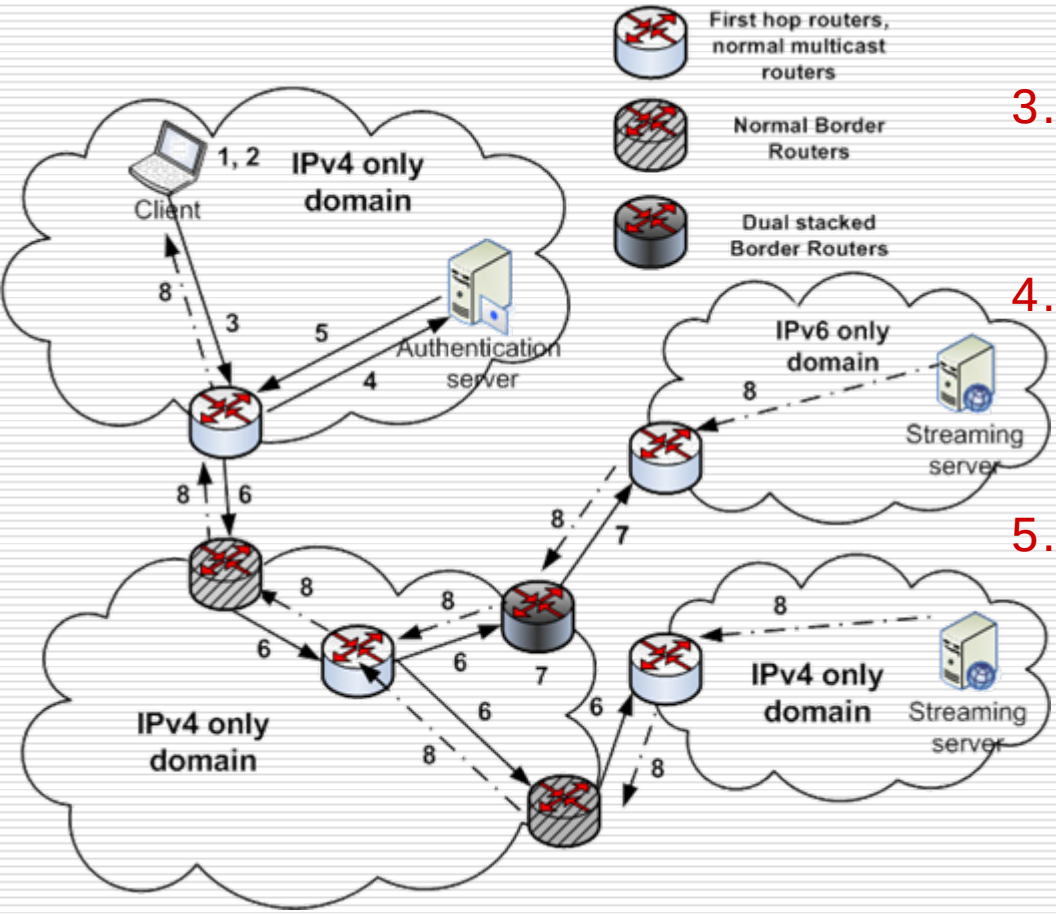


HISM Process

1. Receiver application gives the (HIT-S, SID) couple or the SID information
2. Host Identity layer maps a multicast address from the SID
   - IPv4: 1110 | 11 | 26 bit SID
   - IPv6: FF | FF | fill pattern | SID
   - Subranges of the multicast address range reserved for HISM

A new entry, corresponding to the mapped address, is created in the operating system's registries

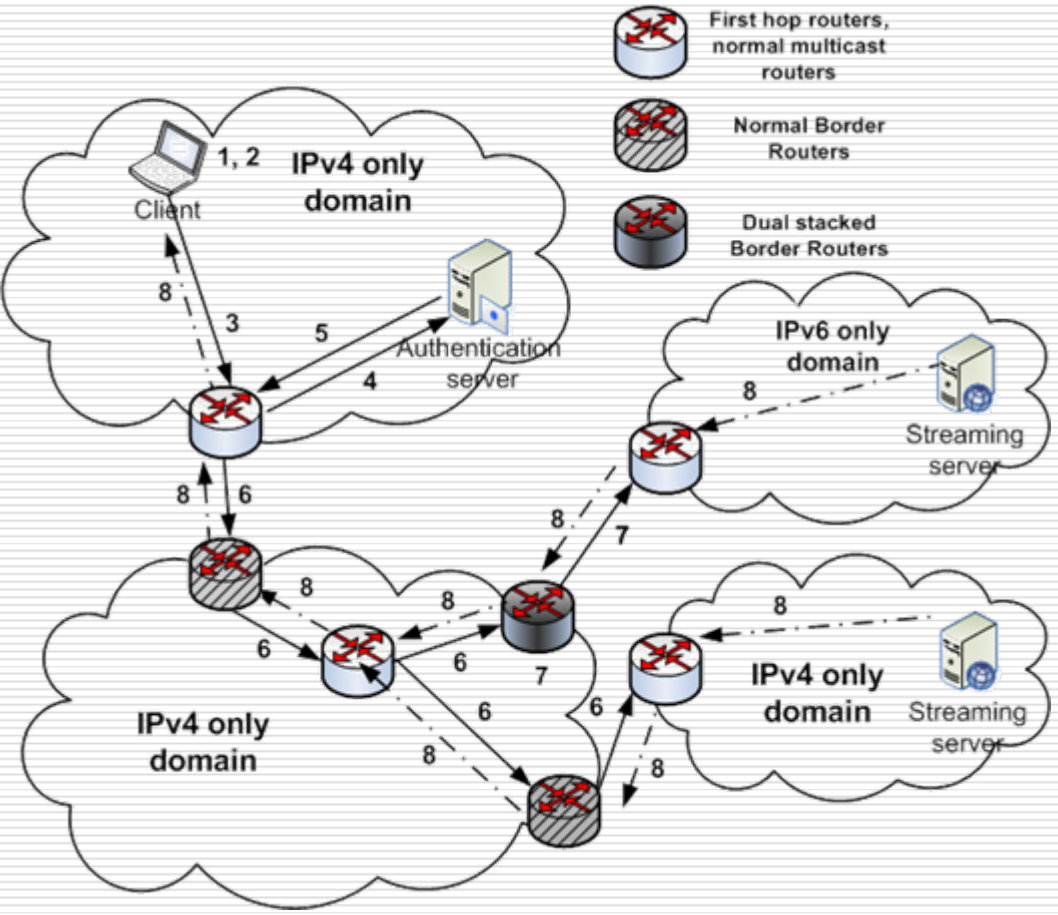
Host Identity Specific Multicast



HISM Process

3. Group management report sent to first hop multicast router (FHR)
   - Contains the HIT-R, HIT-S, SID
4. Authentication and authorization process, based on the HIT-R
   - Is HIT-R allowed to receive (HIT-S, SID)?
5. The authentication server gives back the following information:
   - Client is authorized or not
   - Current Source IP address
     - mapped from the HIT-S
   - IP address of the nearest dual-stacked edge router

Host Identity Specific Multicast



HISM Process

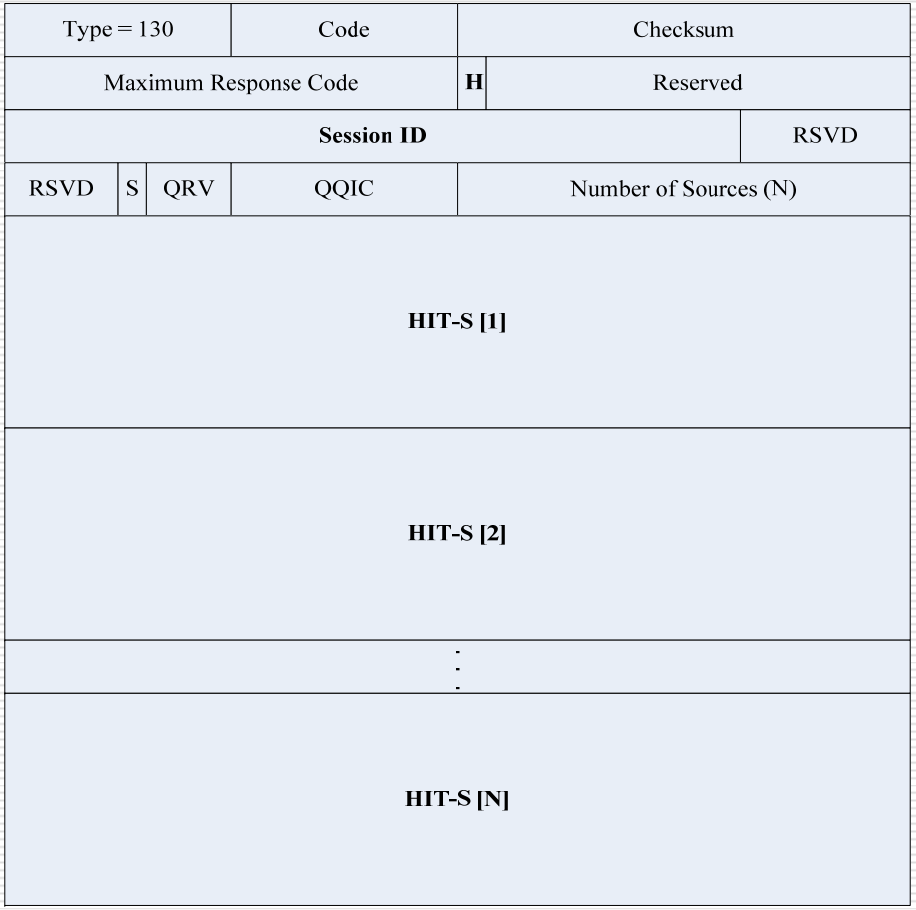
6. If client authorized, the FHR starts the tree building process
   - Sends PIM Join towards the source, if IP versions match
   - Sends PIM join towards the dual-stack edge router, if not
7. Dual-stack edge router handles the IP version conversion and starts building the other part of the multicast tree
   - Sends PIM join towards the source
8. The Join reaches the source's FHR, or an on-tree router
   - multicast data starts flowing on the new tree branch

Modifications to be done

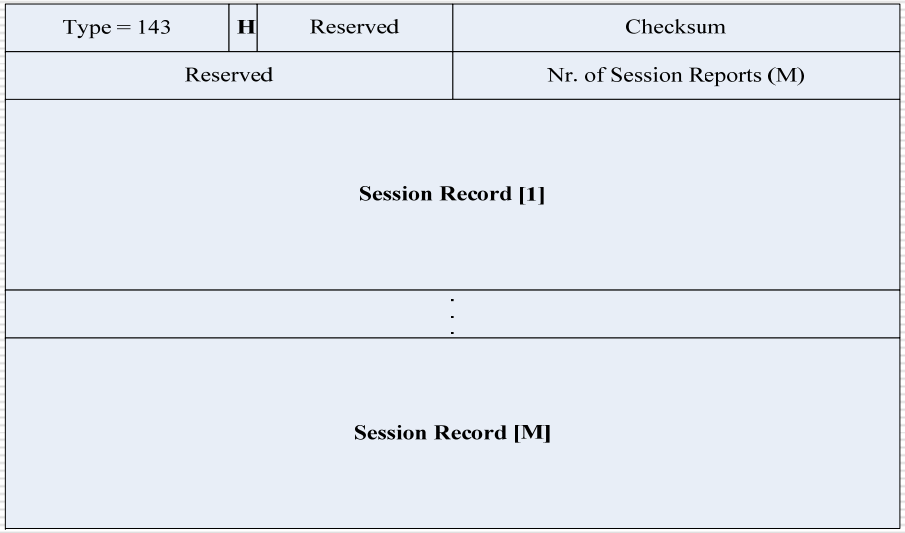
- Application level
  - Application should be capable of handling HITs and SIDs
  - Special reserved address range for HISM
- Group management issues
  - IGMP for IPv4, MLD for IPv6
  - New unified group management for both IPv4, IPv6 that also supports the HISM model
    - VIGMP (Version Independent Group Management Protocol)
      - Client must give it's HIT-R for authentication
  - Support for (HIT-S, SID), (*, SID), (S, G) and (*, G) addressing

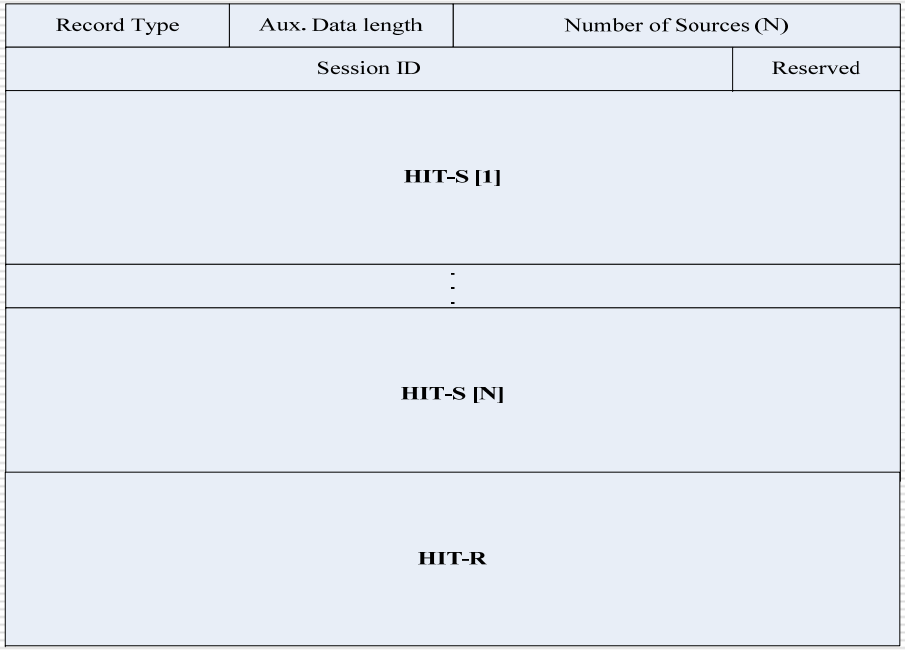
VIGMP Query

- Hosts that do not implement VIGMP can still understand
  - Reply with IGMP (v4) or MLD (v6) Reports
  - VIGMP hosts reply with VIGMP Report
- The H flag denotes HISM compatibility
  - Replaces a reserved bit, not checked by „old” hosts
- Multicast Address → SID
- Source Address → HIT-S



VIGMP Report





- H flag signalling the HISM compatibility
- Session Records contain the multicast session information

- VIGMP Session Record
  - Multicast Address → SID
  - Source Address → HIT-S
  - Additionally contains the HIT-R

Modifications to be done

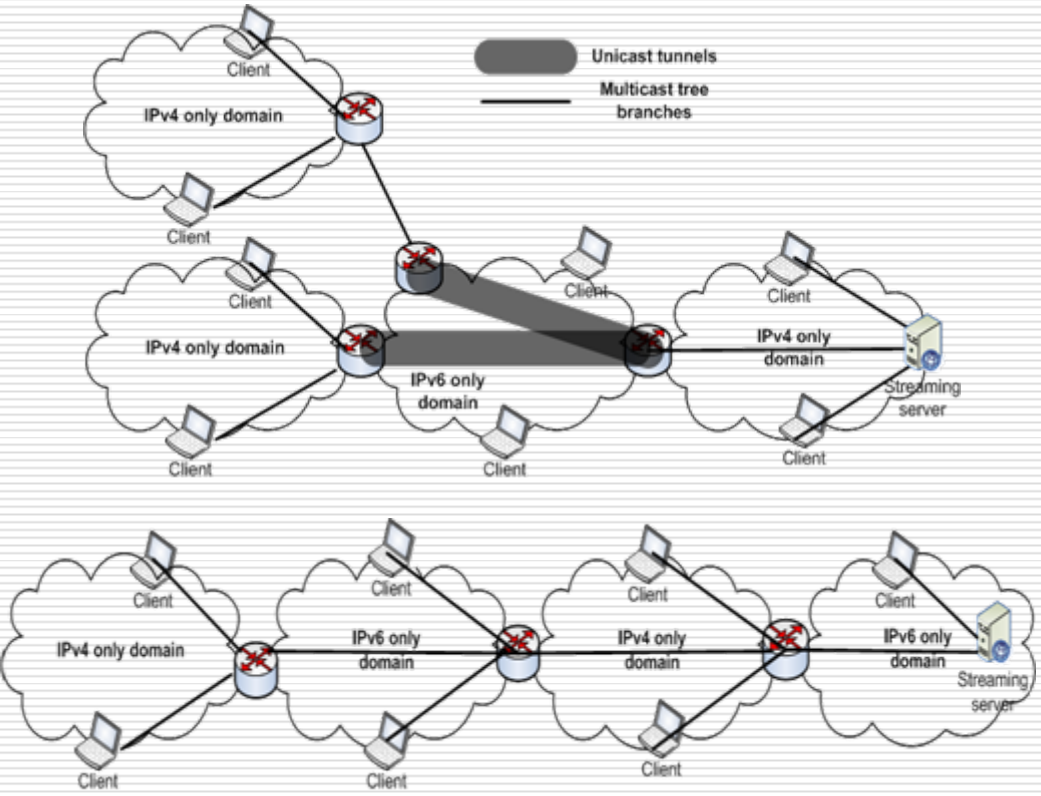
- Multicast routing - Extension to the PIM-SSM protocol
  - First hop router functions
    - Handling of the new group management messages
    - Initiating the authentication process
    - Initiating the tree building process
  - Core PIM routing
    - New identifiers used for maintaining multicast trees:
      - SIDs, HITs

HIT-S	SID	Input interface	Output interface

      - No rebuilding if the source address changes
        - E.g., new IP address on the same subnet, given by DHCP
    - No HIP stack in the core routers
      - Source IP address is the destination address of PIM Join messages
      - The tree is built based on the IP addresses

Modifications to be done

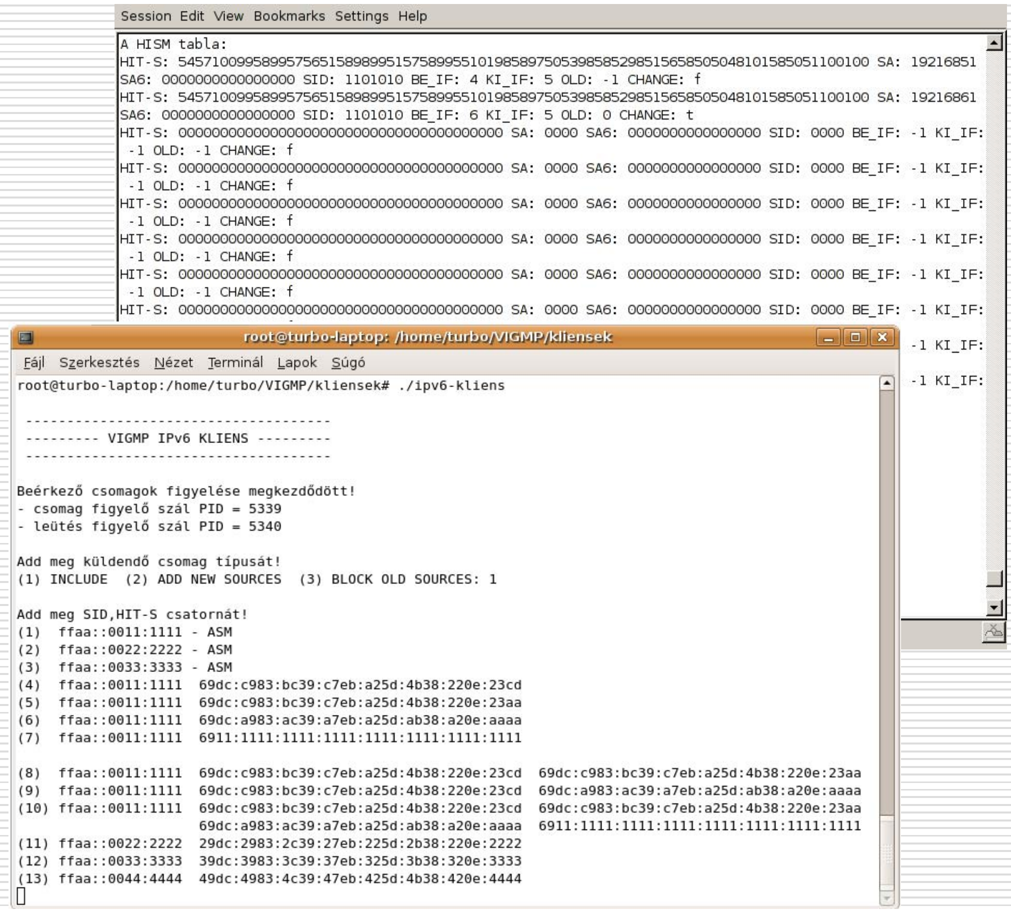
- Dual-stack border routers



- Clients in domains with different IP versions can join the same tree with the help of dual-stack border routers
  - Translate the tree building messages
  - Translate all multicast data on the way back to the clients
- Native dual-stacked multicast trees can be built
  - No tunneling is needed

Test implementations

- VIGMP software
  - C code under Linux
  - Fully functional
- PIM-HISM software
  - C code under Linux
  - Fully functional
- Test client software
- Authentication software
  - Only test version



Summary

- A new multicast model: Host Identity Specific Multicast (HISM)
  - Support for native dual-stacked multicast trees
  - A new unified group management protocol
  - Provides authentication functionalities
  - No tree rebuilding if addresses change

For more information...

- Zsolt Kovacshazi, Rolland Vida, "Host Identity Specific Multicast", in Proc. of Third International Conference on Networking and Services (ICNS 2007), Athens, Greece, June 2007.
  - Received Best Paper Award
- Comments are welcome to vida@tmit.bme.hu