

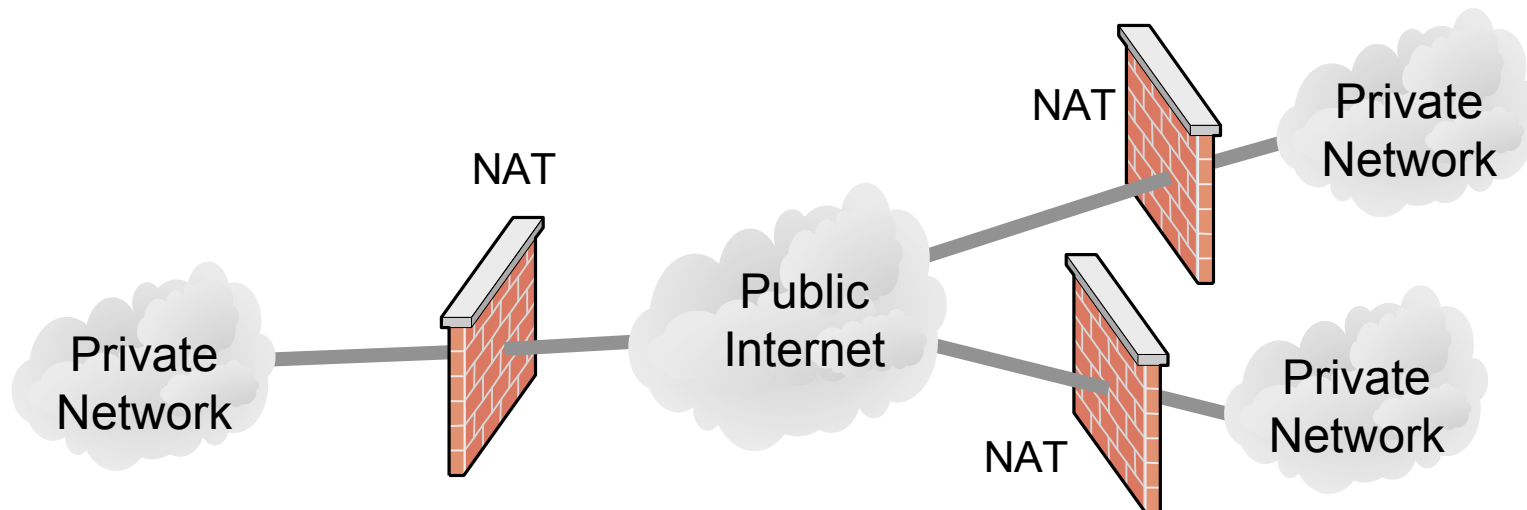
# HIP and NAT

<draft-stiemerling-hip-nat-00.txt>

Martin Stiemerling, Juergen Quittek  
{stiemerling|quittek}@netlab.nec.de  
59th IETF meeting, HIPRR BOF

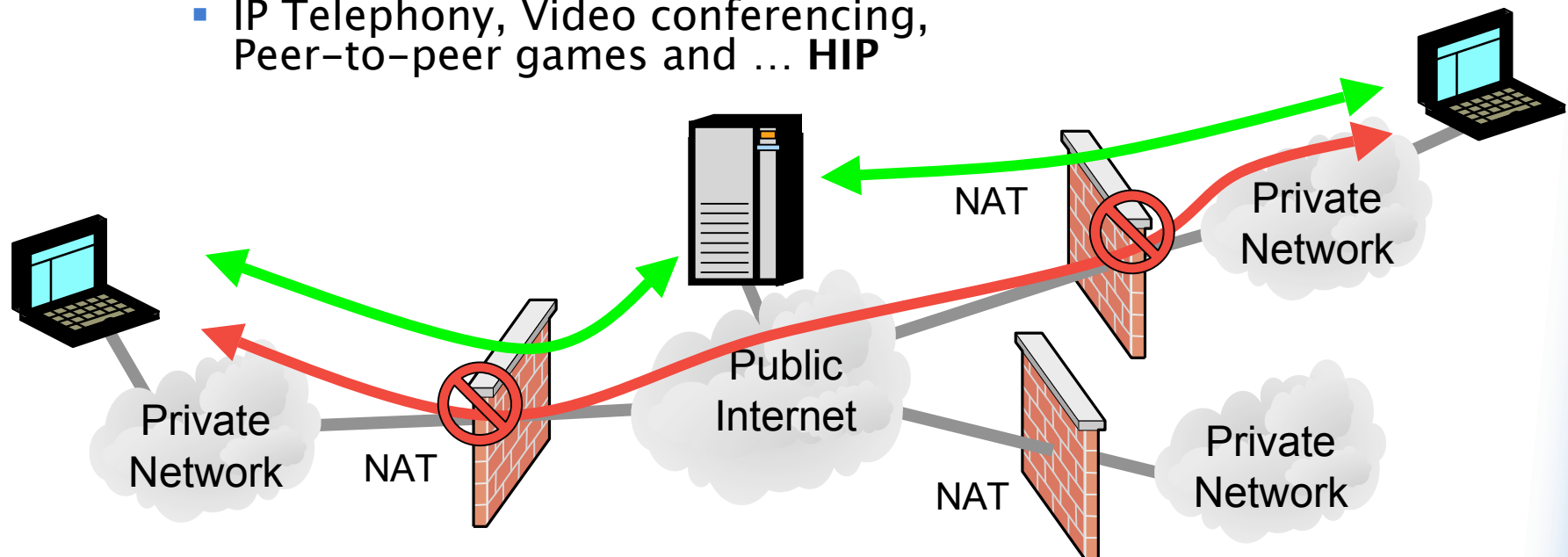
# Network Address Translators

- Network Address Translators are integral components of the Internet
  - ◆ can multiplex many private IP addresses into few public IP addresses
    - typically: port-based multiplexing (probably not required for IPv6)
  - ◆ block traffic from the outside (rather a firewall function)
  - ◆ hide internal network structure
  - ◆ enable flexible network renumbering
    - change of ISP (without internal renumbering)
    - change of private network addressing (without notifying ISP, public DNS)
- NATs are not just IPv4-specific
  - ◆ even organizations owning IPv4 class A network address spaces use NATs



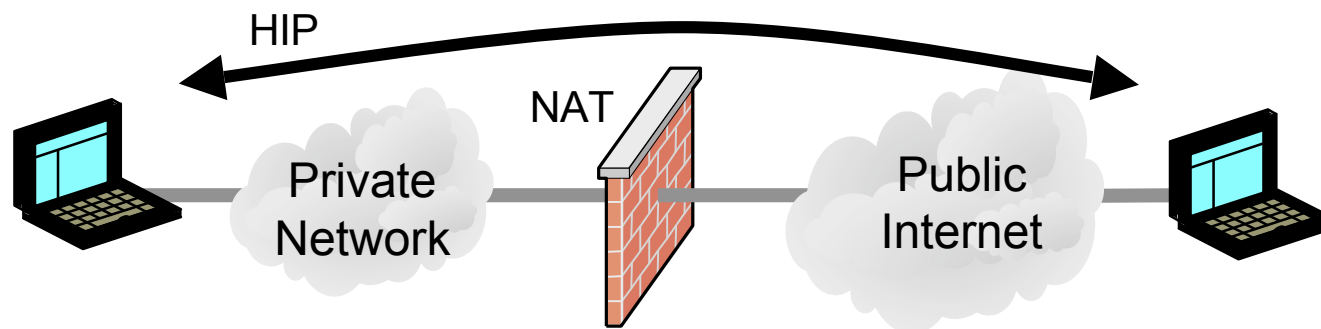
# The NAT Problem

- Applications using fixed port numbers can pass Firewalls and NATs with static configuration
  - ◆ Particularly **client-server** applications
    - HTTP, SMTP, FTP, SSH
- Firewalls and NATs block applications that choose port numbers dynamically
  - ◆ Particularly **peer-to-peer** applications
    - IP Telephony, Video conferencing, Peer-to-peer games and ... **HIP**



# Problems with HIP Base Exchange

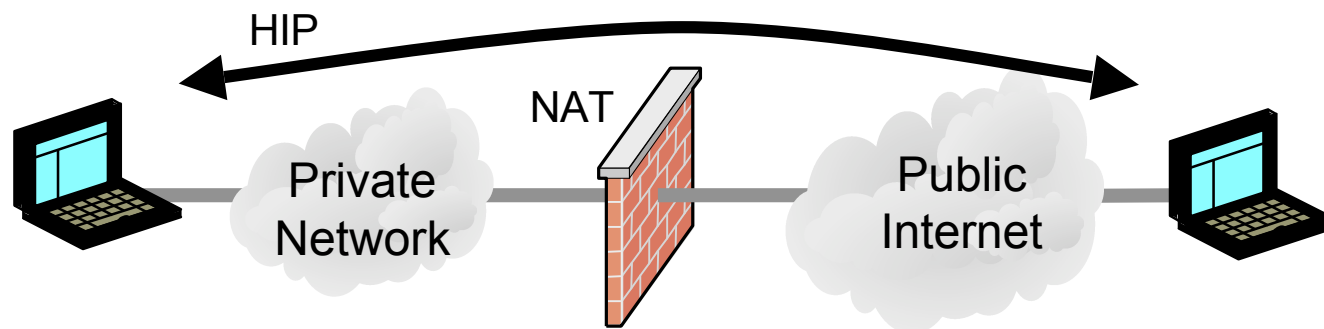
- HIP Transport
  - ◆ IPv6: in specific extension header
  - ◆ IPv4: as IP payload or as UDP payload
- Scenario 1: Base exchange initiated in private network
  - ◆ IPv6 and IPv4 using IP payload do not work with current (multiplexing) NATs
    - NATs do create state for TCP/UDP ports and ICMP codes
    - They need to be extended to do the same for HITs
    - would work well with non-multiplexing (IPv6) NATs
  - ◆ IPv4 over UDP works, but not if source port is fixed (to 272)



# Problems with HIP Base Exchange

Scenario 2: Base exchange initiated in public network

- Public IP address at NAT need to be known
  - ◆ Could be handled by rendezvous server
    - Needs to be considered when designing rendezvous protocol
- multiplexing NATs need to be extended to support HIT multiplexing



# Problems with IPsec Transport (1)

- All known problems of IPsec apply
  - ◆ See draft-ietf-ipsec-nat-reqts-06.txt
- ESP-only works through NAT, AH does not
- But: NAT breaks TCP/UDP checksums
  - ◆ NAT changes content of pseudo header without changing checksum
  - ◆ checksum 'hidden' in ESP payload
- Solution: send pseudo header information in base exchange
  - ◆ similar to suggestion in draft-ietf-ipsec-nat-t-ike-08.txt for IKE
  - ◆ using original header when checking checksums
  - ◆ potential security problem: disclosure of internal address

# Problems with IPsec Transport (2)

- Multiplexing NATs need to support IPsec SPI multiplexing
  - ◆ Outbound SPI value independent of inbound SPI value
- NATs must learn corresponding outbound and inbound SPI values
- NATs could monitor HIP base exchanges
  - ◆ Processing overhead
- Signalling Protocol
  - ◆ Use of protocols, such as NSIS or MIDCOM protocols (or NAT MIB?) to tell NAT about SPIs
    - see nsis and midcom WG charters

# Problems with REA

- REA packet exchange to notify about external address
  - ◆ REA: draft-nikander-hip-mm-01.txt
- REA packet contains sending host's IP address(es)
- Receiver needs to get the sending host's public address(es) at the NAT
- Solutions:
  - ◆ NAT translates REA messages
    - (too?) strong requirement for NAT
  - ◆ Sending host already sends its public address at the NAT
    - Problem: How to obtain the external address?
    - Solution: Could use MIDCOM or NSIS protocols (or NAT MIB) or STUN (RFC 3489, needs to be extended for this application)