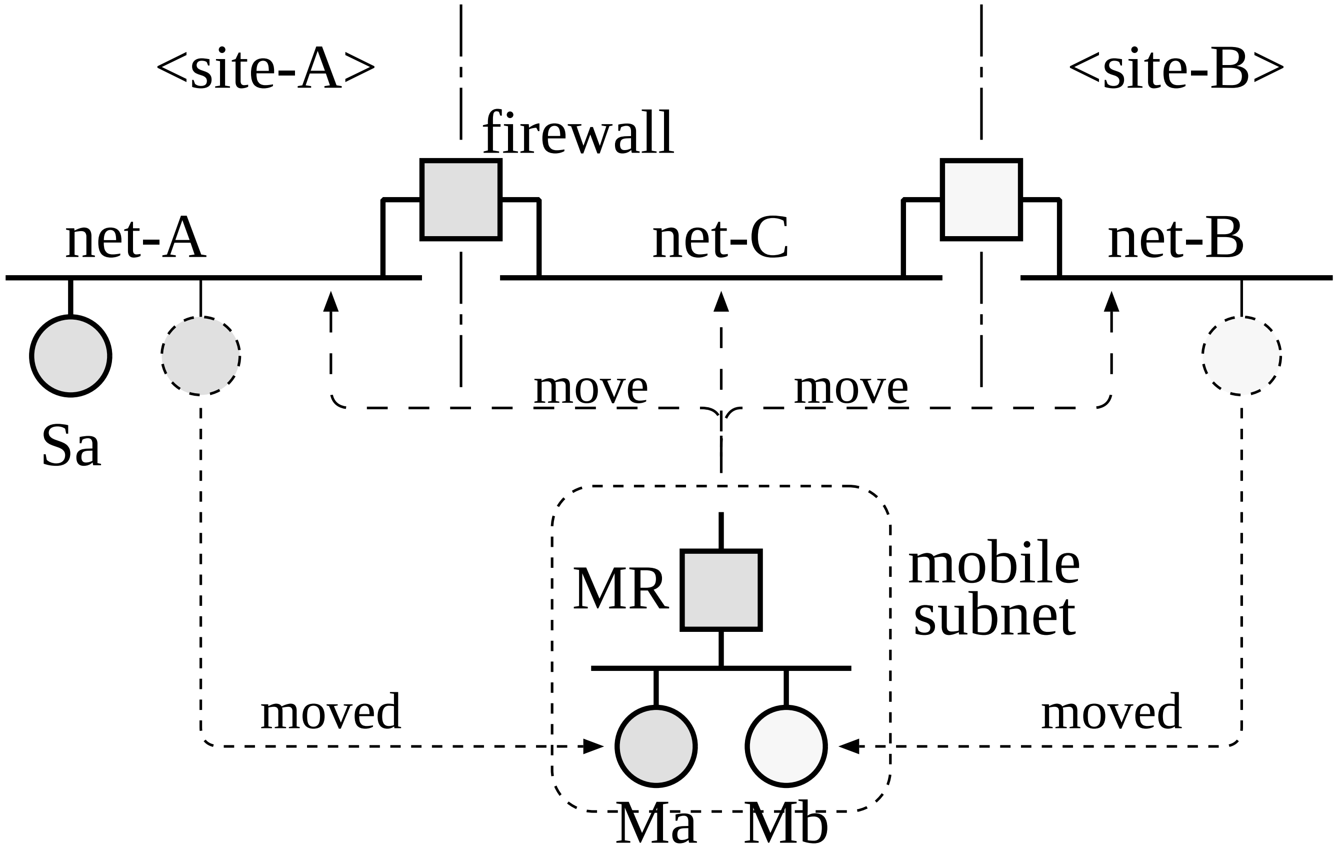
Authentic Firewall Traverse
and
Subnet Mobility
in
VIPv3

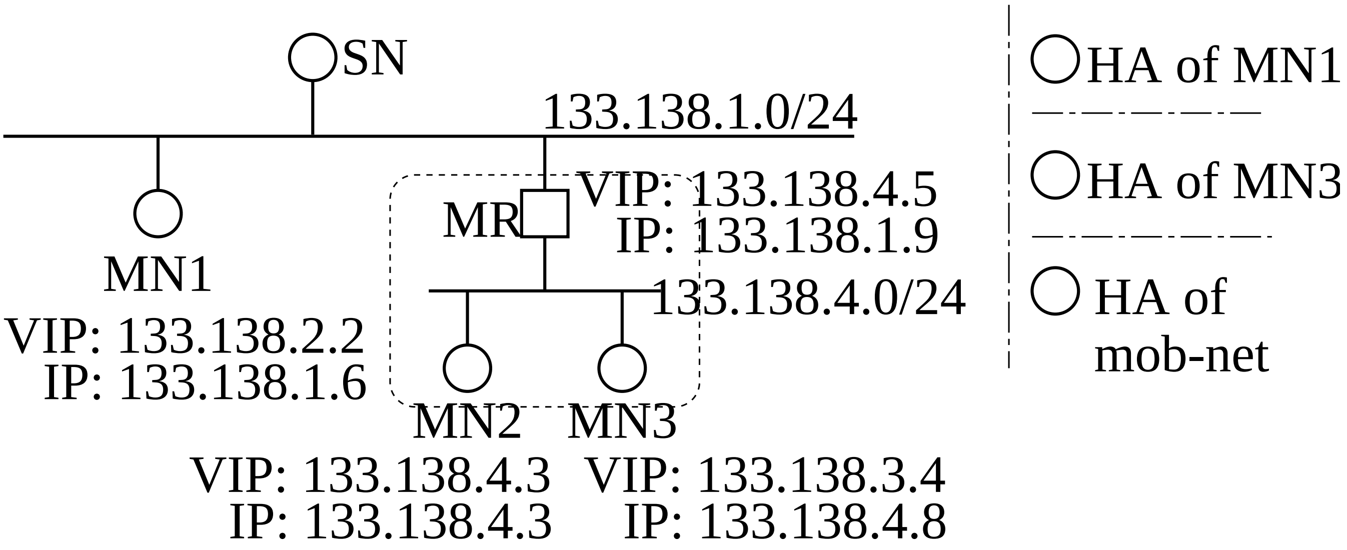
Fumio Teraoka
tera@csl.sony.co.jp
Sony Computer Science Laboratory Inc.

Test Network



- Ma and Mb can transparently move among net-A, net-B, net-C, and the mobile subnet.
- The mobile subnet can also transparently move among net-A, net-B, and net-C.
- Ma can communicate with Sa via the firewall while Mb cannot.
  - The firewall authenticates the source node.
- Mb cannot impersonate Ma.

Mechanism for Subnet Mobility

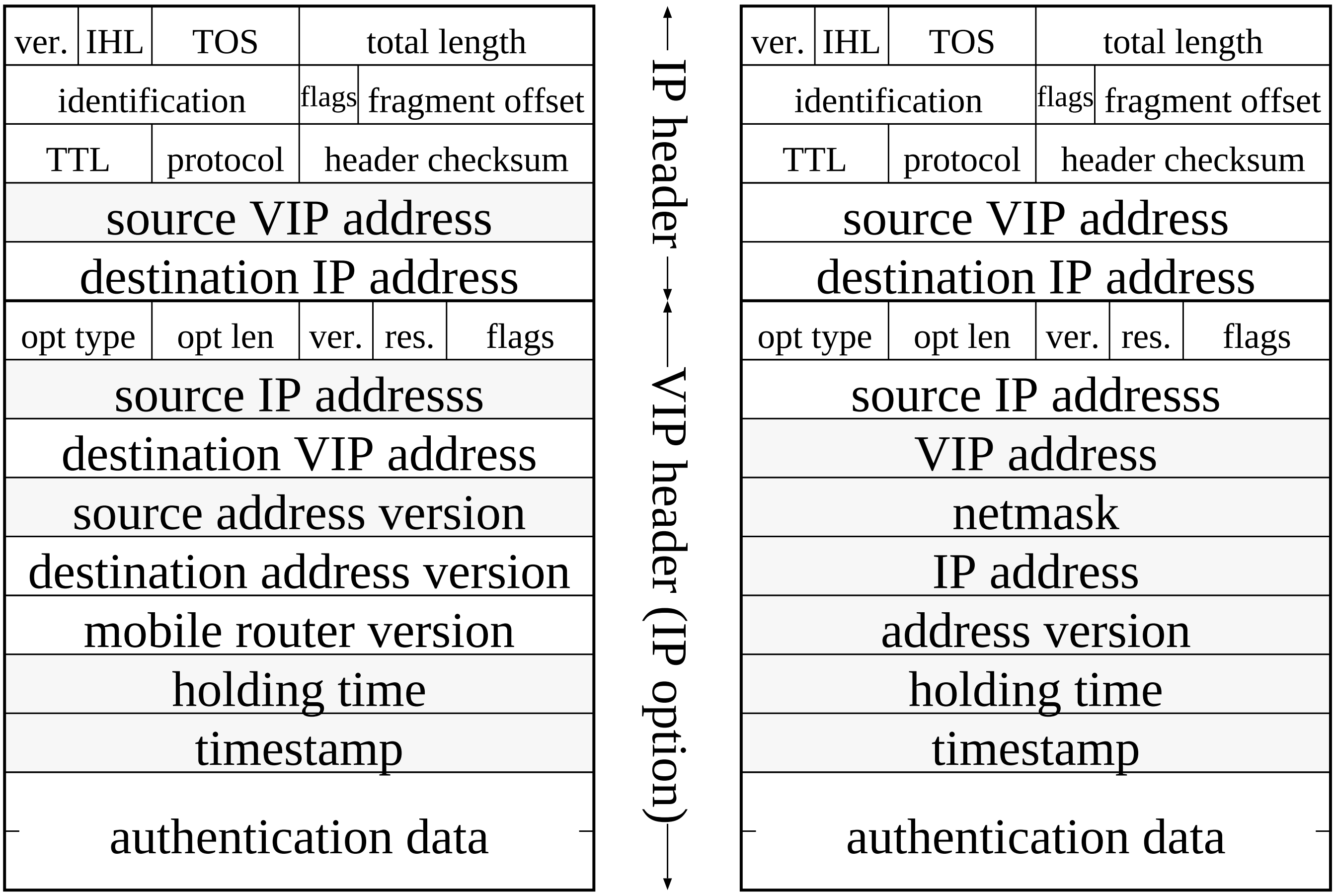


<AMT entries>

133.138.2.2	133.138.3.4	133.138.4.5	133.138.4.0
0xffffffff	0xffffffff	0xffffffff	0xffffff00
133.138.1.6	133.138.4.8	133.138.1.9	133.138.1.9
for MN1	for MN3	for MR	for mob-subnet

- **node mobility (VIPv1 and v2)**
  - **IP address specifies the location.**
  - **“VIP address” is introduced as ID.**
  - **Address Mapping Table (AMT) for efficient mapping.**
- **subnet mobility (VIPv3)**
  - **netmask is introduced in AMT.**

Packet Format



ver. | IHL | TOS | total length
identification | flags | fragment offset
TTL | protocol | header checksum
source VIP address
destination IP address
opt type | opt len | ver. | res. | flags
source IP addresss
destination VIP address
source address version
destination address version
mobile router version
holding time
timestamp
authentication data

(a) data packet

ver. | IHL | TOS | total length
identification | flags | fragment offset
TTL | protocol | header checksum
source VIP address
destination IP address
opt type | opt len | ver. | res. | flags
source IP addresss
VIP address
netmask
IP address
address version
holding time
timestamp
authentication data

(b) control packet

- **each VIPv3 packet has the ID of the source node and authentication data.**
- **keyed MD5 with 128-bit key is used.**
- **firewall can authenticate the source node if both nodes share a secret key.**

Current Status

- VIPv3 is running on BSD/OS-2.1.
  - kernel modification
    (size: 774.2KB to 788.6KB)
  - authentication daemon
  - some commands
- processing overhead of keyed MD5
  - 22 μsec on P5-166
  - 76 μsec on i486-DX4 75MHz
  - negligible
- VIPv2 (not v3) is distributed.
  - ftp://ftp.csl.sony.co.jp/CSL/vip-dist/vip204-bsdos210.tar.gz