Fast Authentication for Secure Internet Service

Kenji FUJIKAWA (ROOT Inc.)

Hitoshi MORIOKA (ROOT Inc.)

Hiroshi MANO (ROOT Inc.)

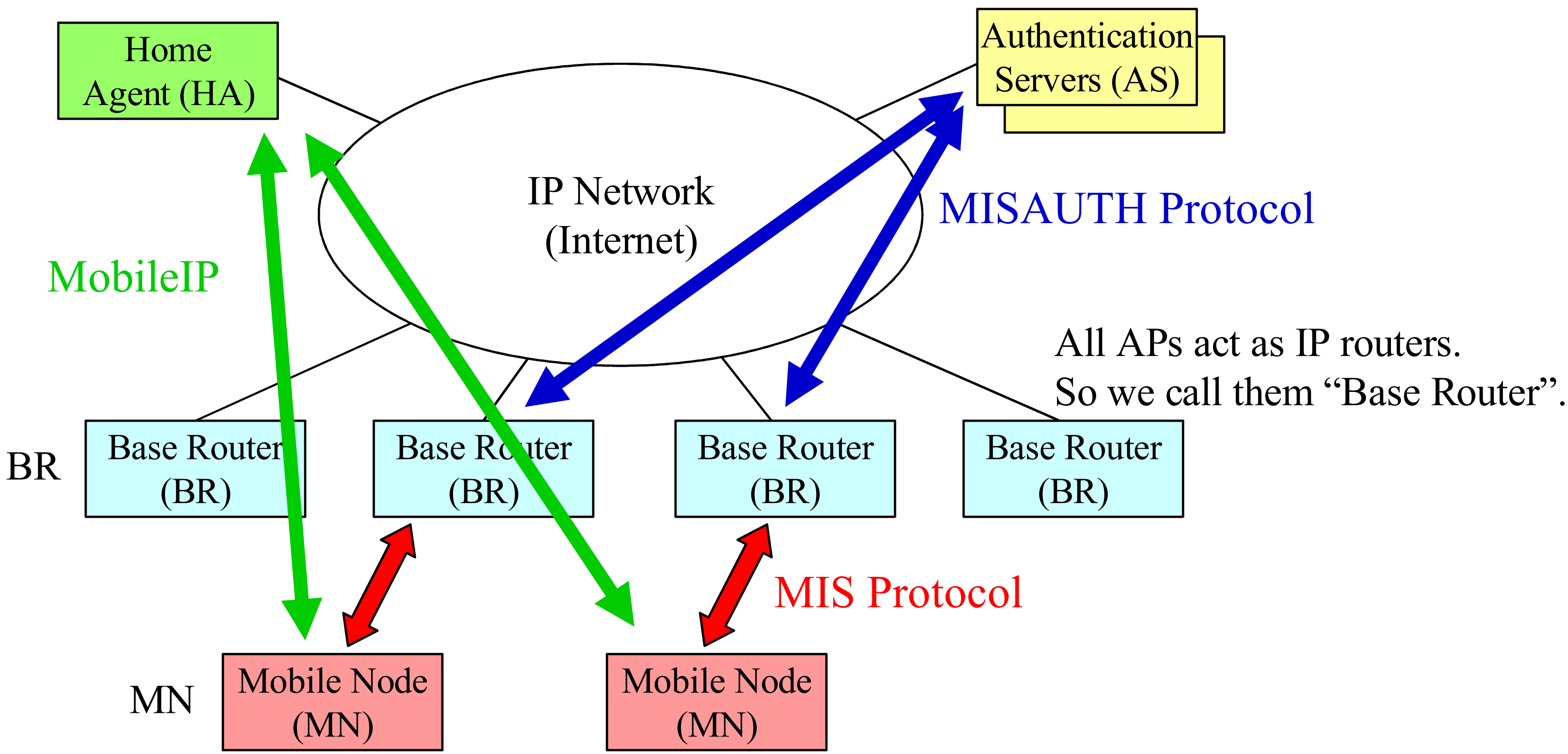
Overview

- **Introduce our MIS Protocol (MISP), a fast authentication protocol on wireless LAN**
- **Comparison with IEEE802.11 and IEEE802.1x from the point of view of handover latency**
- **Comparison with IEEE802.11 and IEEE802.1x from the point of view of security**

Introduction

- **The combination of Wireless LAN and mobile IP is a fast and low-cost mobile communication method.**
- **But there are some issues.**
  - Security Weakness
  - Handover Latency
- **So we developed a new link layer protocol, MISP.**
- **MISP is also adaptable to UPKI or MIAKO.Net**

MIS System Architecture



Hitoshi MORIOKA, ROOT Inc.

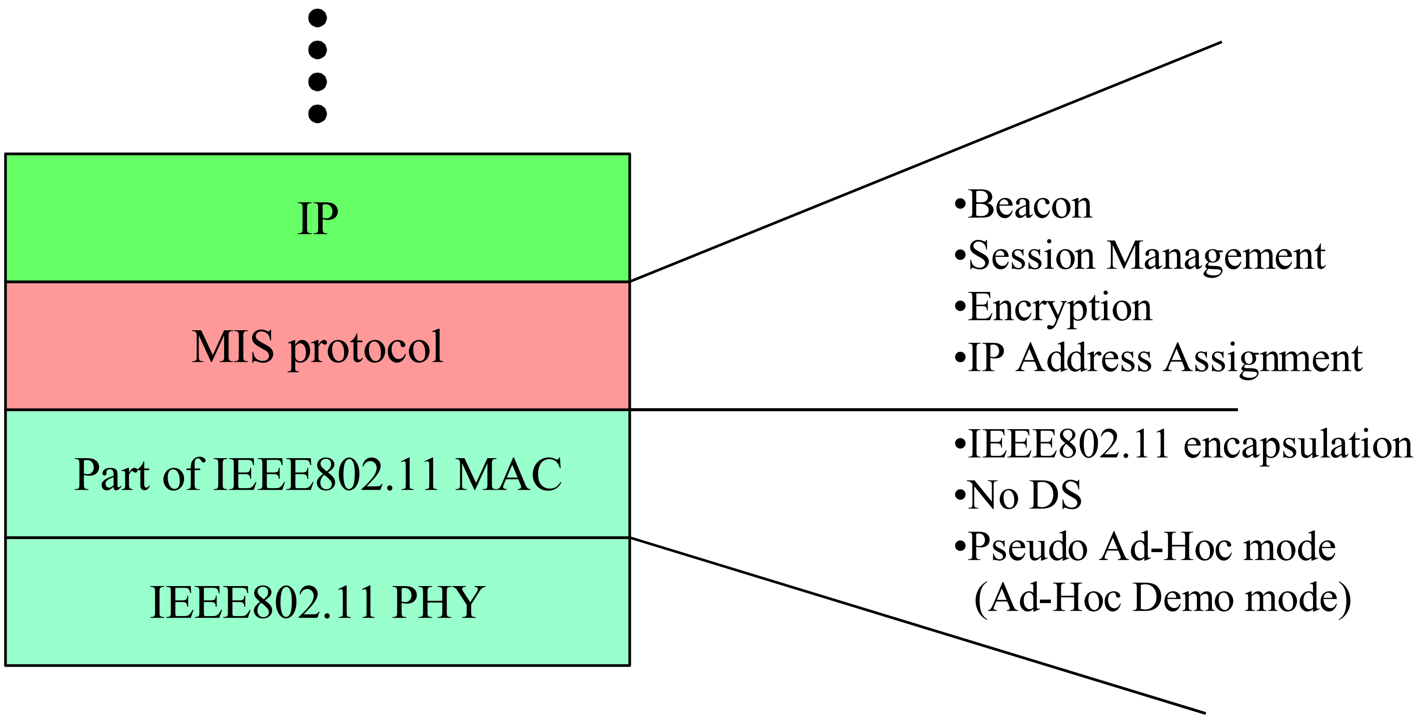
MISP Overview

- **MIS protocol is a layer 2 protocol designed for public mobile internet services.**
- **IPv4/IPv6 are targets as upper layer.**
- **Lower layer is IEEE802.3 or part of IEEE802.11.**
- **Features**
  - Mutual authentication, session key exchange and network layer setup between a base router (BR) and a mobile node (MN) by ONE ROUNDTRIP PACKET EXCHANGE

    Effective for fast handover
  - Encryption between AP and STA with periodic key update
  - Authentication of every frame
  - Multiple Service Providers support
- **It can be used with MISAUTH protocol (MISAUTHP) which enables remote authentication over IP.**
  - based on RADIUS

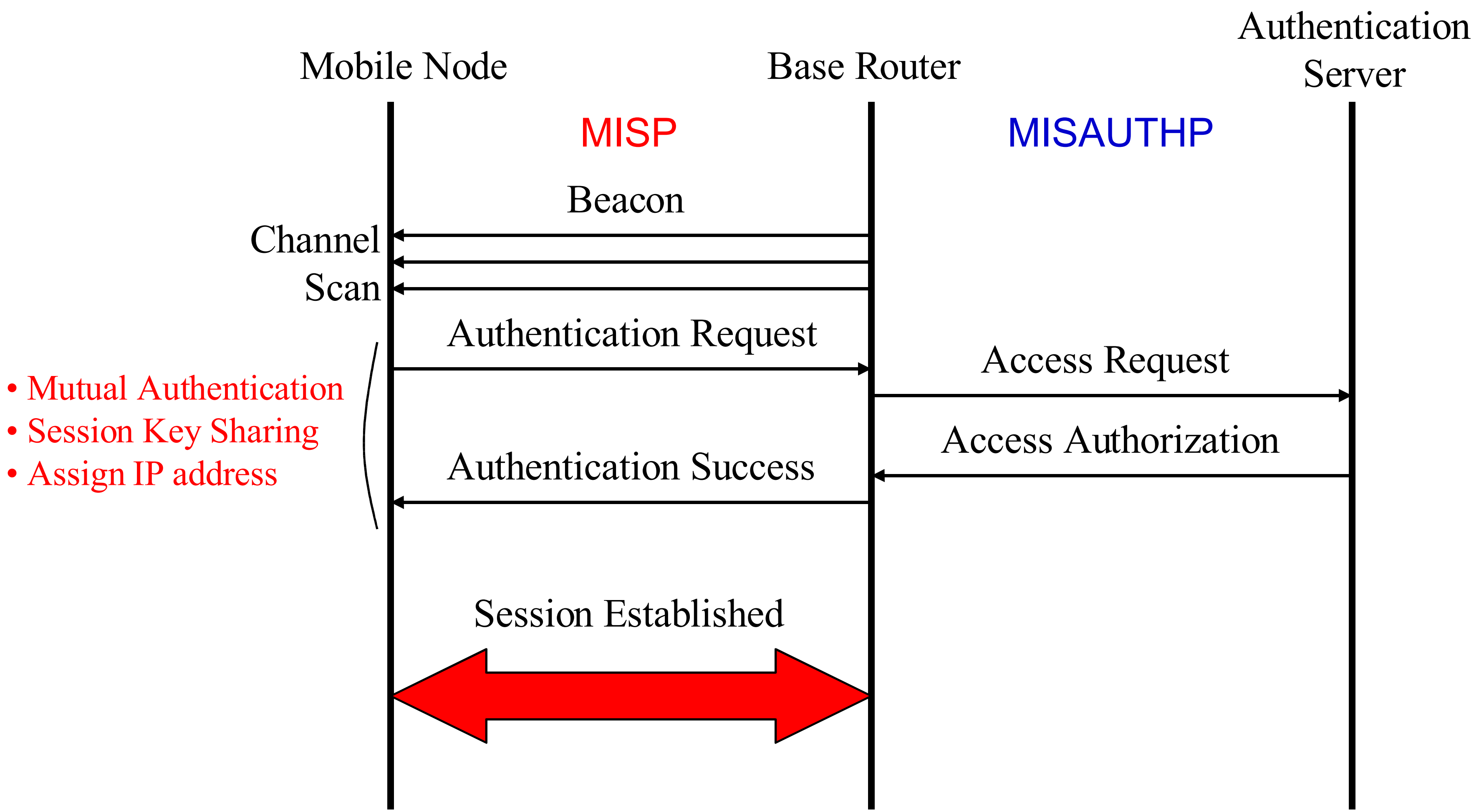
Layer

In case of using IEEE802.11 as lower layer



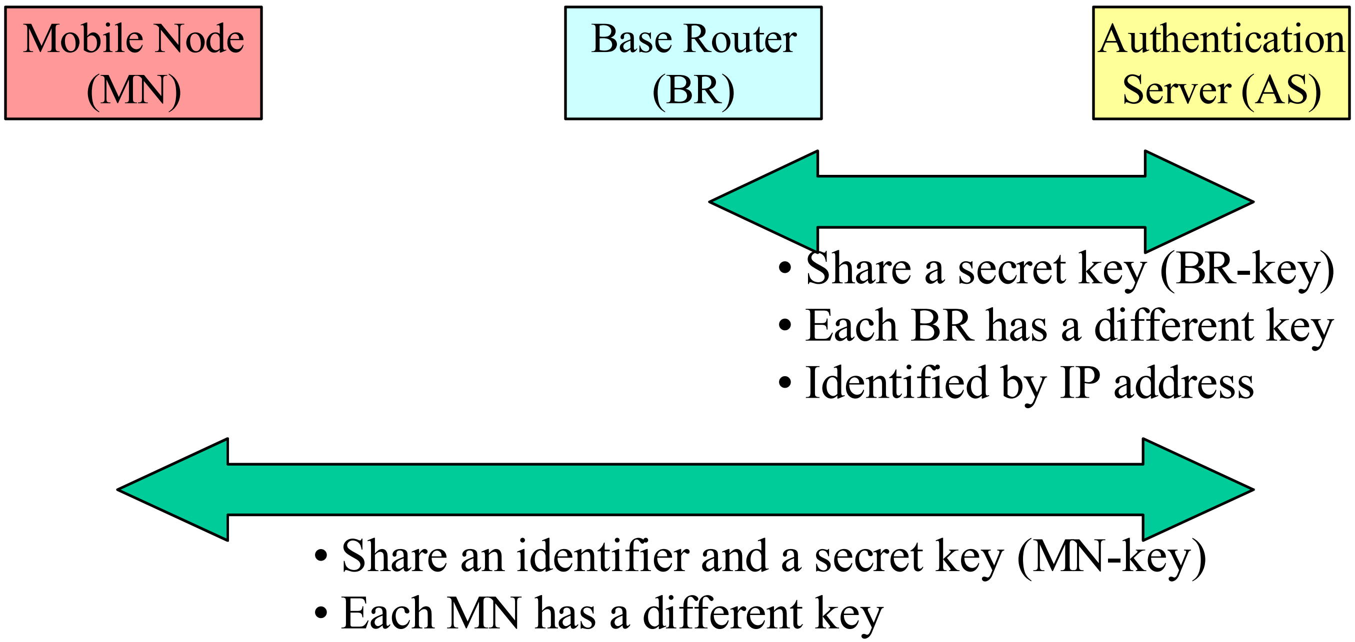
Hitoshi MORIOKA, ROOT Inc.

MISP and MISAUTHP Sequence



Hitoshi MORIOKA, ROOT Inc.

Pre-shared Secret Key



- **No pre-shared information between MN and BR**

Hitoshi MORIOKA, ROOT Inc.

MIS Protocol Frame Format

- MIS Protocol Control Frame

IEEE802.11 Header	IEEE802.2 Header	MISP Control Message

- MIS Protocol Data Frame (transferring network layer packet)

IEEE802.11 Header	IEEE802.2 Header	MISP Header	IP Header	••••

Encrypted
by MISP

- Ethernet number 0x8893 is assigned for MISP by IEEE.

MIS Protocol Control Message Format

MISP Header

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Code	Flags	Length

Control Message

Code	Message
0x00	Data
0x01	Beacon
0x03	Authentication Request
0x04	Authentication Success
0x08	Authentication Fail
0x09	Finish Session

- Followed by some "objects"

Format of an Object

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Type	Length	Value…

Objects

Type	Length	Name	Beacon	Auth. Req.	Auth. Suc.	Auth. Fail
0x00	1	Padding	Optional	Optional	Optional	Optional
0x02	10	Beacon Timestamp	Required	Required	Required	Required
0x03	6	IPv4 Local Address		Optional	Optional	
0x04	6	IPv4 Remote Address			Optional	
0x05	Variable	ICV (Integrity Check Value)		Required	Required	
0x06	Variable	NAI (Network Access Identifier)		Required		
0x08	Variable	Session Key Derivery Data		Required		
0x09	14	Geographical Information	Optional			
0x0a	3	IPv4 available address number	Optional			
0x0b	3	IPv4 Source Address Filter	Optional			
0x0d	4	Error Reason				Required
0x0e	2+4n	BR Group	Required			
0x0f	4	Session Key Valid Time			Required	
0x10	4	Serial Number	Required			
0x11	4	Beacon Interval	Required			
0x12	2+2n	Security Type	Required	Required		
0x13	8	Uplink Speed	Optional			
0x14	3	Channel	Optional			
0x15	2+2n	Network Layer Type	Required	Required	Required	

Security Types Supported by MISP

- **Null (Optional)**
  - No security
- **HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit (Optional)**
  - HMAC-MD5 is used for authentication.
  - HMAC-MD5 is used for delivery of session key.
  - HMAC-MD5 is used for authentication of frame.
- **HMAC-MD5/HMAC-MD5/AES-CBC-128bit (Mandatory)**
  - HMAC-MD5 is used for authentication.
  - HMAC-MD5 is used for delivery of session key.
  - AES-CBC-128bit is used for data encryption

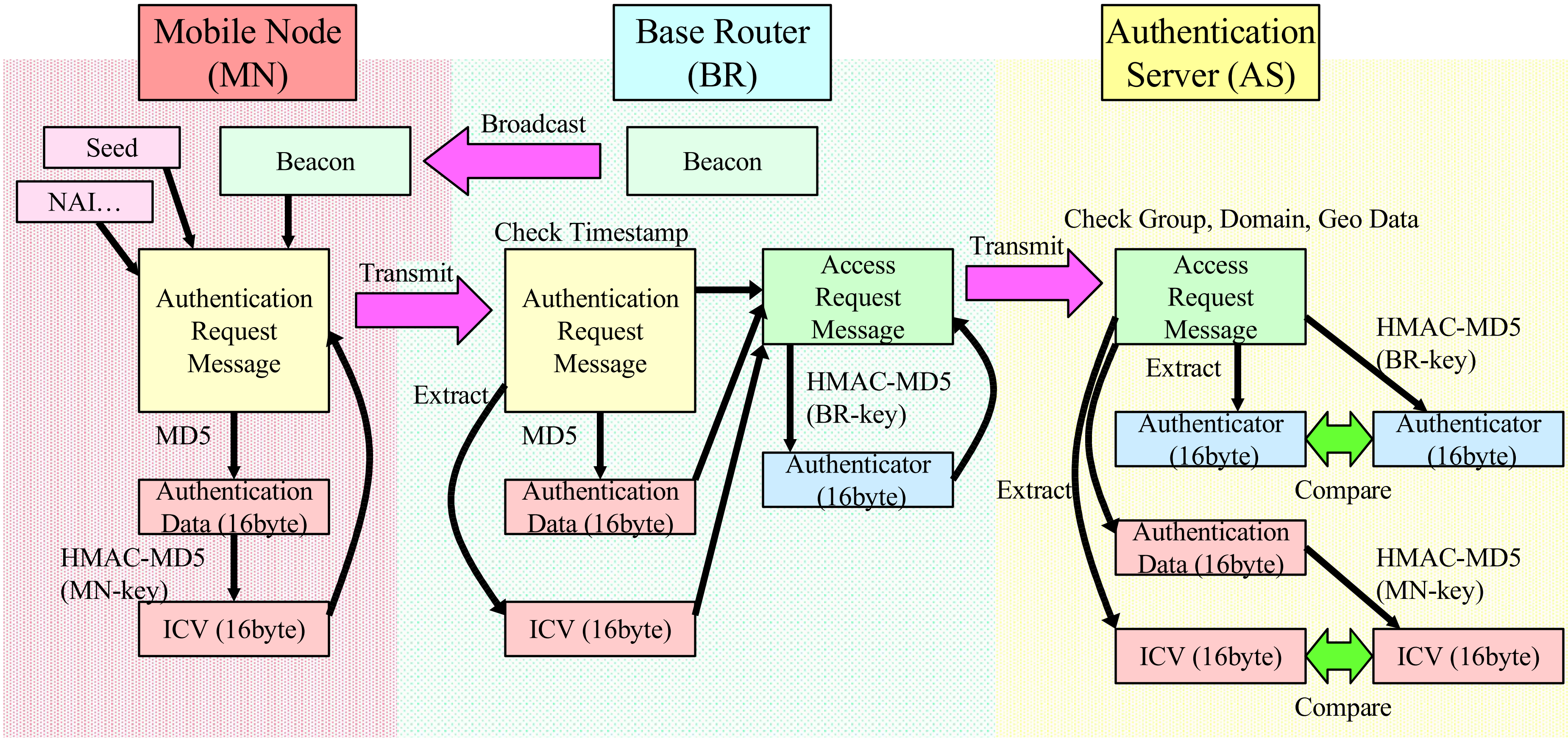
Beacon

- **Beacons are transmitted in 30ms interval.**
- **Each beacon includes the following information.**
  - Timestamp
  - Serial number
  - Beacon interval
  - Group (like SSID)
  - Supported Network layer type
  - Remaining IPv4 addresses
  - Channel
  - Etc…

Behavior of MN

1. **An MN makes a list of BRs by scanning channels and receiving beacons. The BRs in the list have corresponding "group (like SSID)".**
2. **The BR list is sorted by the signal strength of the beacon.**
3. **The MN try to authenticate to the top of the list of BRs.**
4. **If the authentication fails, the MN try to authenticate to the next BR in the list until the end of the list.**
5. **After the authentication succeed, the MN can communicate to the network.**
6. **The MN makes a registration to the HA.**
7. **The MN watches the beacon of connected BR. If the MR cannot receive the beacons of the BR for a certain period or the beacon strength becomes less than the threshold, the MN closes the session and return to 1.**

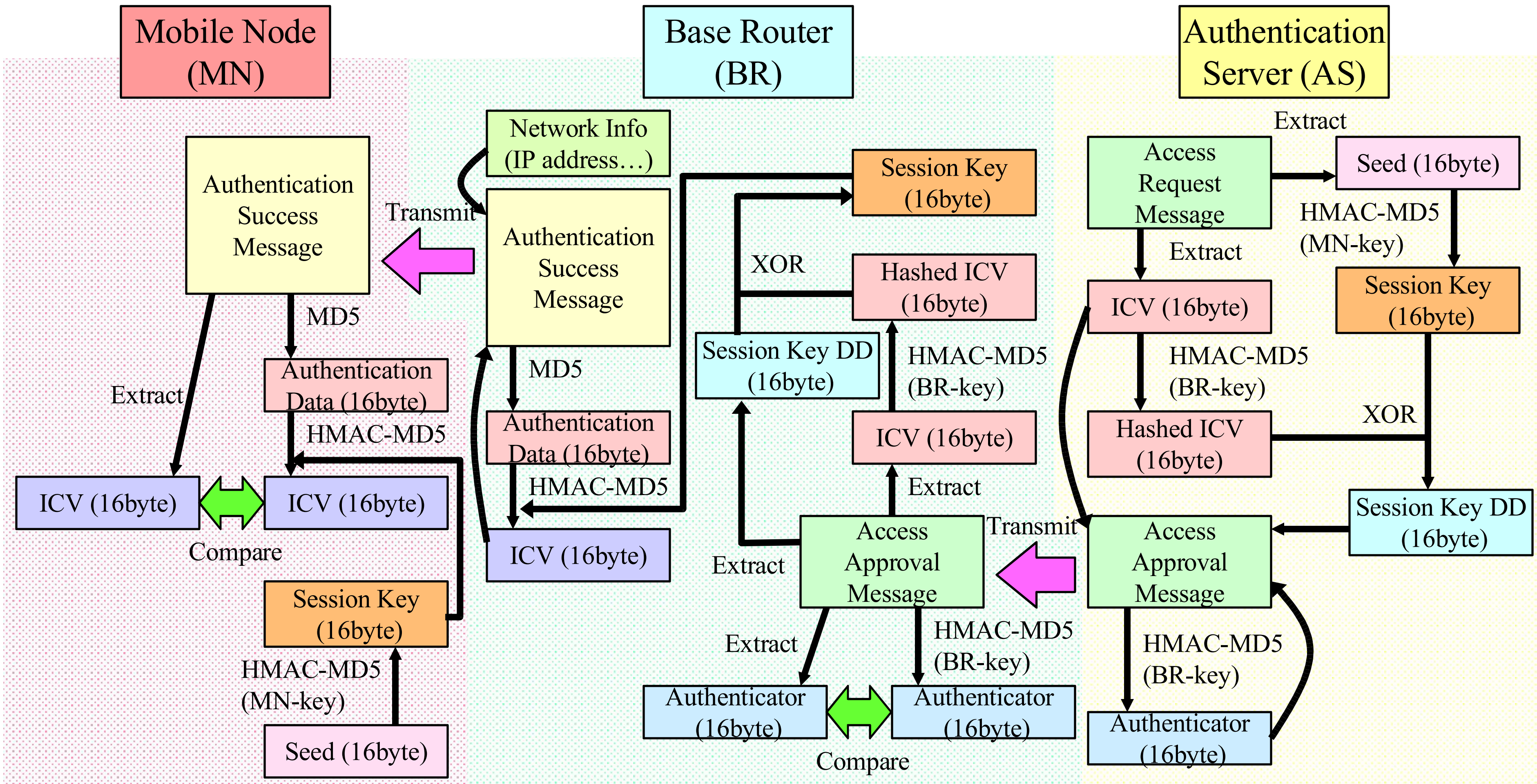
Authentication
(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)



Hitoshi MORIOKA, ROOT Inc.

Authentication (Cont.)

(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)

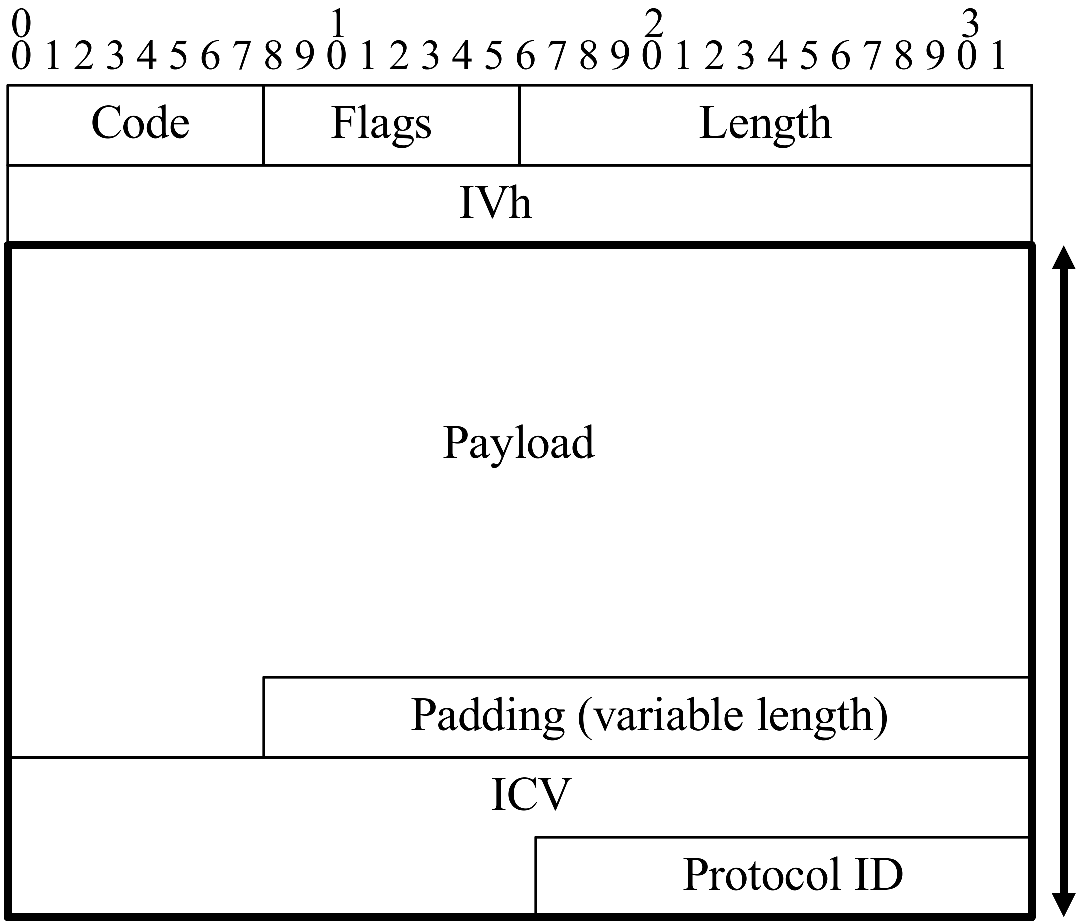


Network Layer Setup

- **IPv4 Configuration**
  - Assign IP address and gateway
  - DNS server, SMTP server, etc. are not assigned because it is premised on mobile IP. In case of using mobile IP, it is enough that fixed servers are installed near the home agent.
  - But it is easy to expand to assign them for non mobile IP users by defining new objects.
- **Other network layer such as IPv6 support is also easy by defining new objects.**

Hitoshi MORIOKA, ROOT Inc.

Data Message Format
(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)



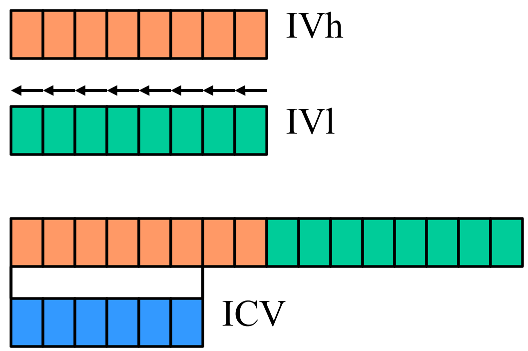
Encrypted Portion

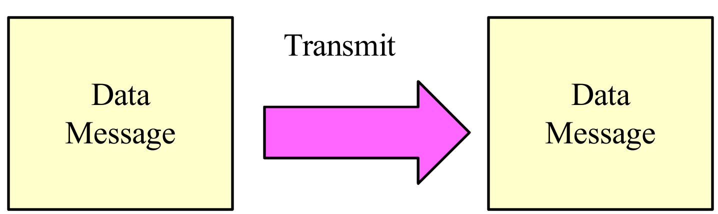
- IVh: Upper 8 octets of the Initialization Vector for AES-CBC
- Payload: A packet data of the upper protocol
- Padding: It makes the payload multiple of 16 octets
- Protocol ID: Indicates the network layer protocol

Encryption, Decryption and Message Authentication (AES-CBC-128bit)

Sender

1. 8 octet IVh is randomly generated.
2. Each octet of the IVh rotate 1bit left. It is IVl.
3. Concatenate IVh and IVl. It is IV.
4. ICV is upper 6 octet of IVh.
5. Encrypt the payload, padding, ICV and Protocol ID by AES-CBC.
6. Make the message by adding MISP header and the IVh.



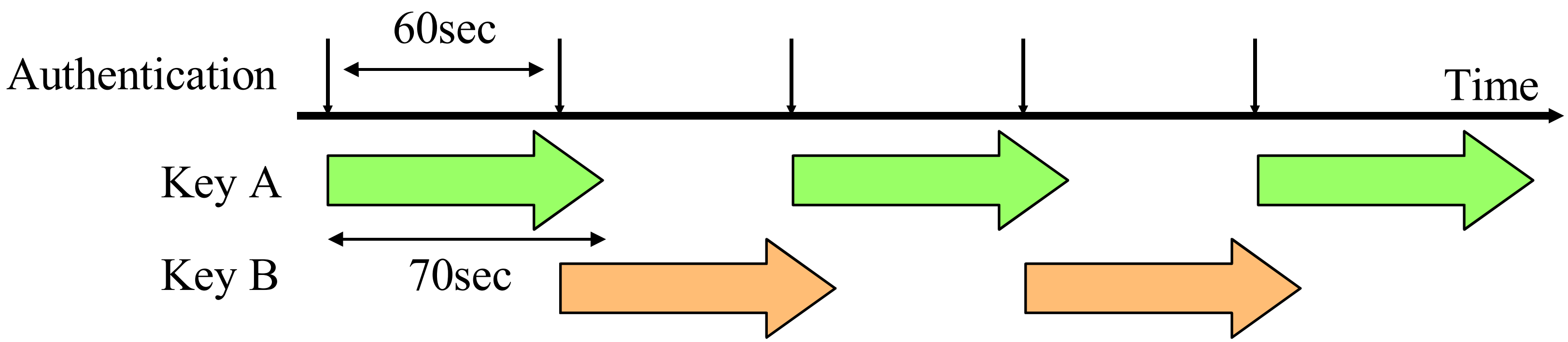


Receiver

1. Extract the IVh from the data message.
2. Each octet of the IVh rotate 1bit left. It is IVl.
3. Concatenate IVh and IVl. It is IV.
4. ICV is upper 6 octet of IVh.
5. Decrypt the data message.
6. Extract the ICV from the decrypted message and compare it to the ICV calculated in 4 to confirm validity.

Hitoshi MORIOKA, ROOT Inc.

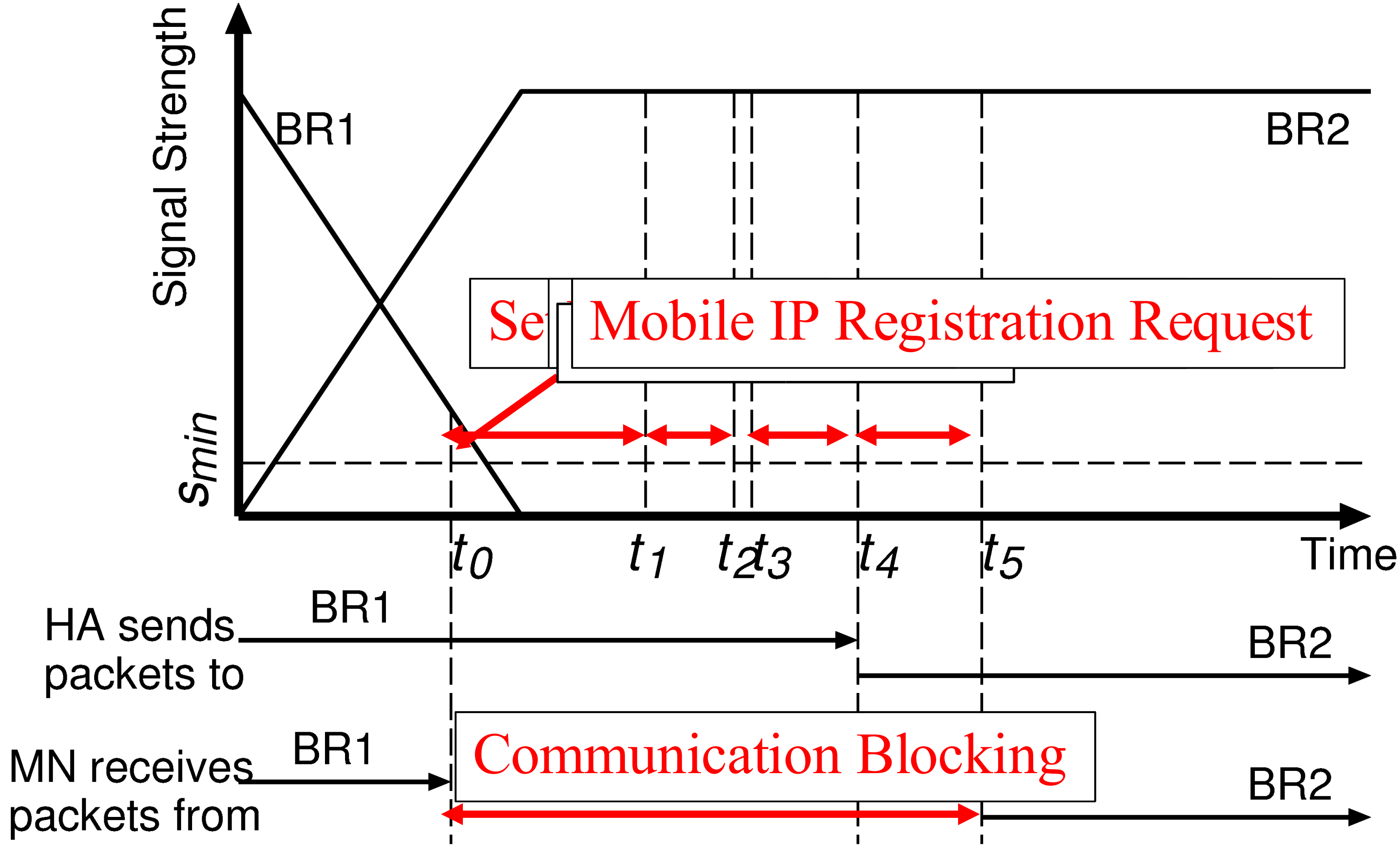
Session Key Updating



• The session key is identified by the flag in the MISP header.

Hitoshi MORIOKA, ROOT Inc.

Communication Blocking in Handover

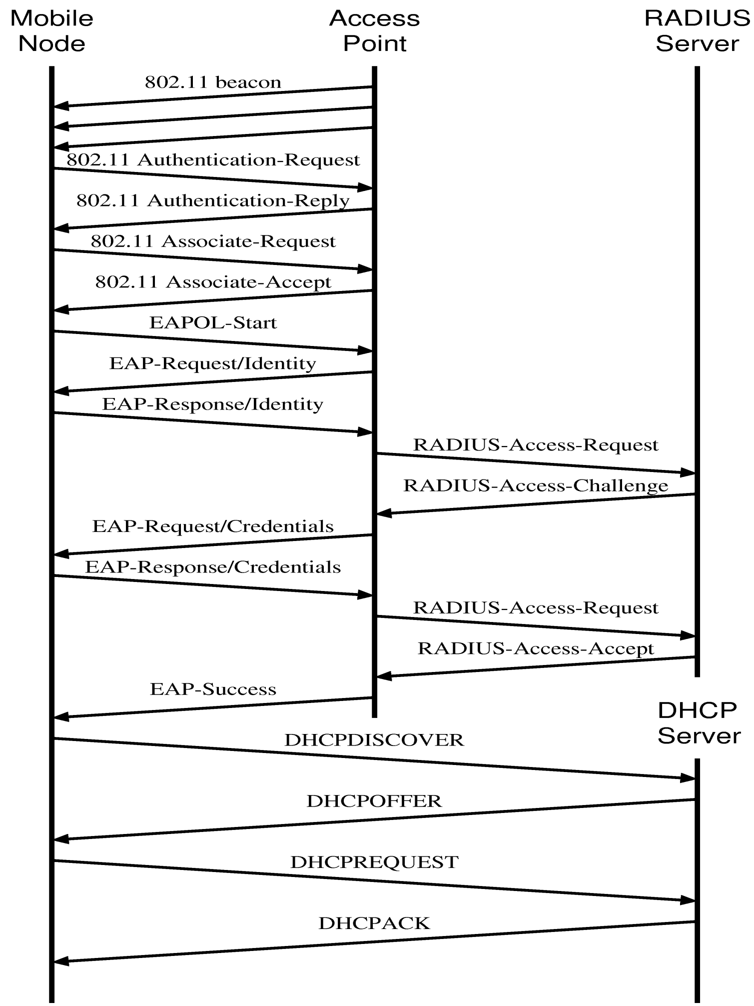


Hitoshi MORIOKA, ROOT Inc.

Factors of Communication Blocking

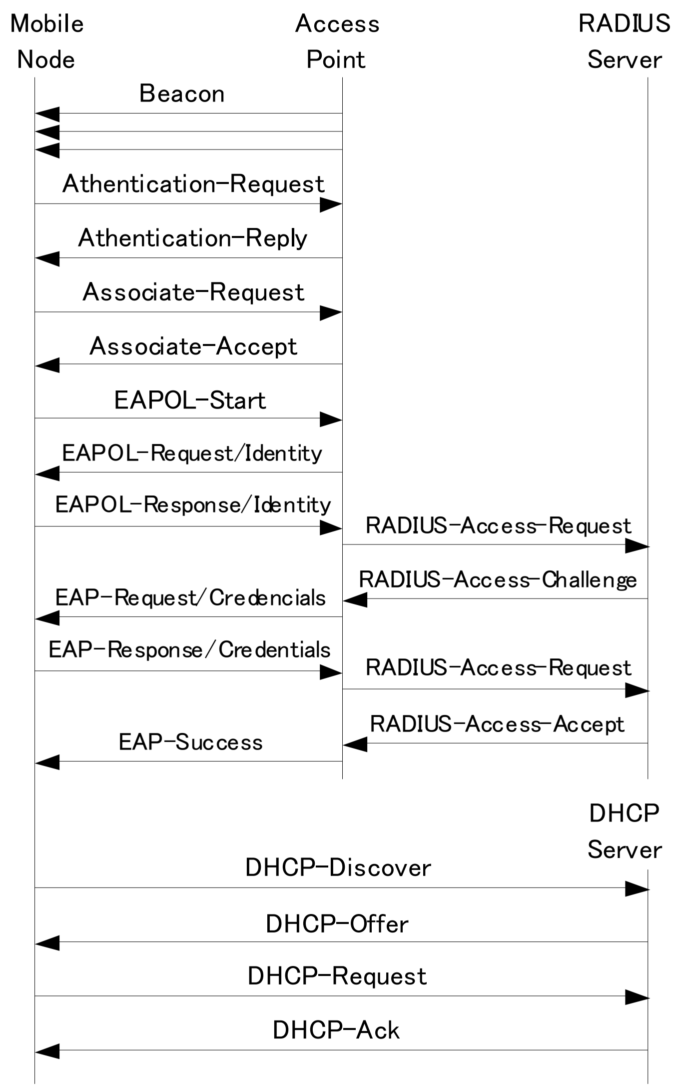
- Channel Scan
- Link Layer Set up
- IP Layer Set up
- Mobile IP registration

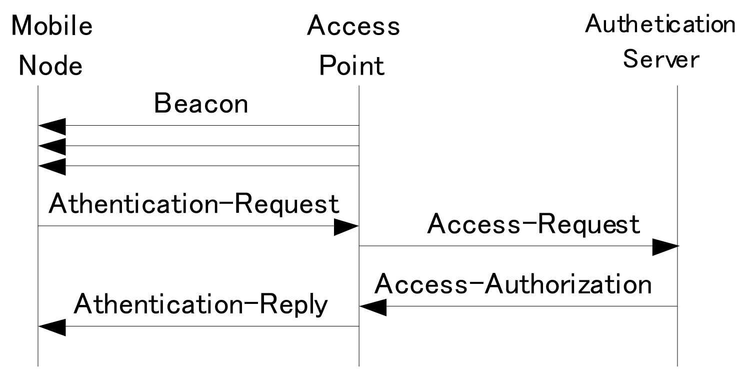
IEEE802.11+IEEE802.1x Session Establishment



- 2 roundtrip packet exchanges between MN and AP for association
- 3 roundtrip packet exchanges between MN and AP for authentication.
- 2 roundtrip packet exchanges between AP and RADIUS server for authentication.
- 2 roundtrip packet exchanges between MN and DHCP server for IP layer set up.

Comparison with IEEE802.11, IEEE802.1x and DHCP





Handover Comparison with IEEE802.11+IEEE802.1x

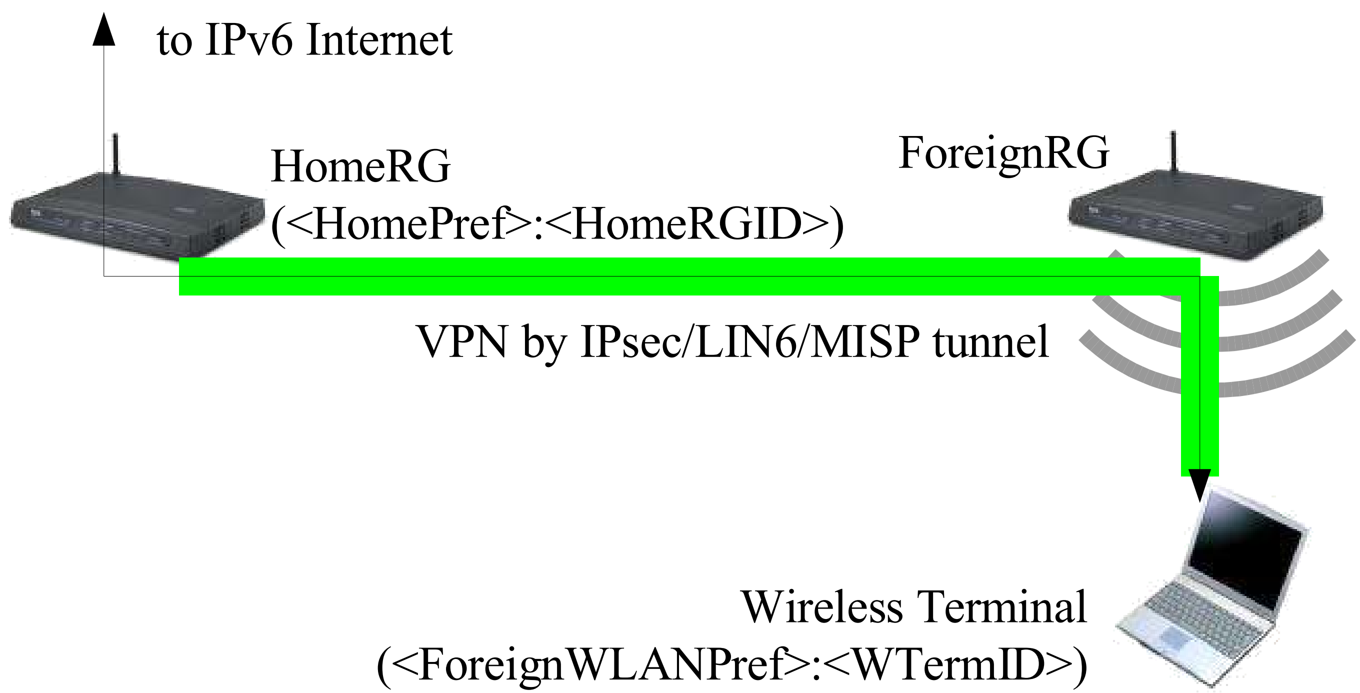
- If the authentication server is far away from BR(AP), the time needed to establish session is significantly affected by the number of packet exchanges.
- And DHCP needs more time to set up IP layer.
- So MISP has advantage to fast handover because it needs only ONE roundtrip packet exchange between MN and BR, and BR and AS to establish session including IP layer set up.

Security Comparison with IEEE802.11+IEEE802.1x

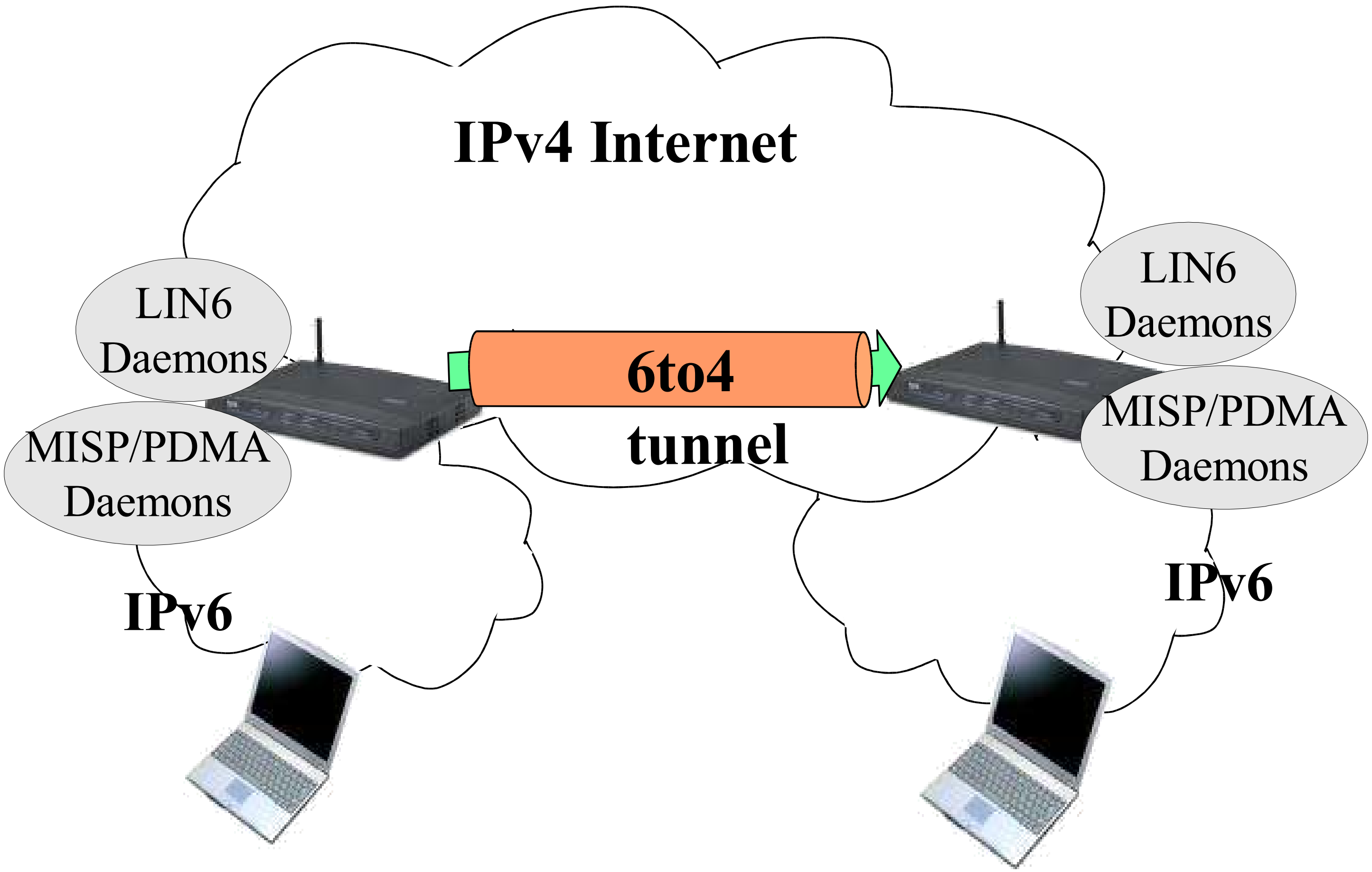
	IEEE802.11+IEEE802.1x	MISP+MISAUTHP
Man-in-the-middle attack	Available by fake EAP success message	Unavailable (avoided by mutual auth.)
Fake access points	Available	Unavailable (avoided by mutual auth.)
DoS attack by fake management frame	Available	Depends on implementation
Session Hijack	Available by MAC address hijacking	Unavailable (avoided by packet auth.)

Most Recent Reseach
VPN by IPsec6/LIN6/MISP

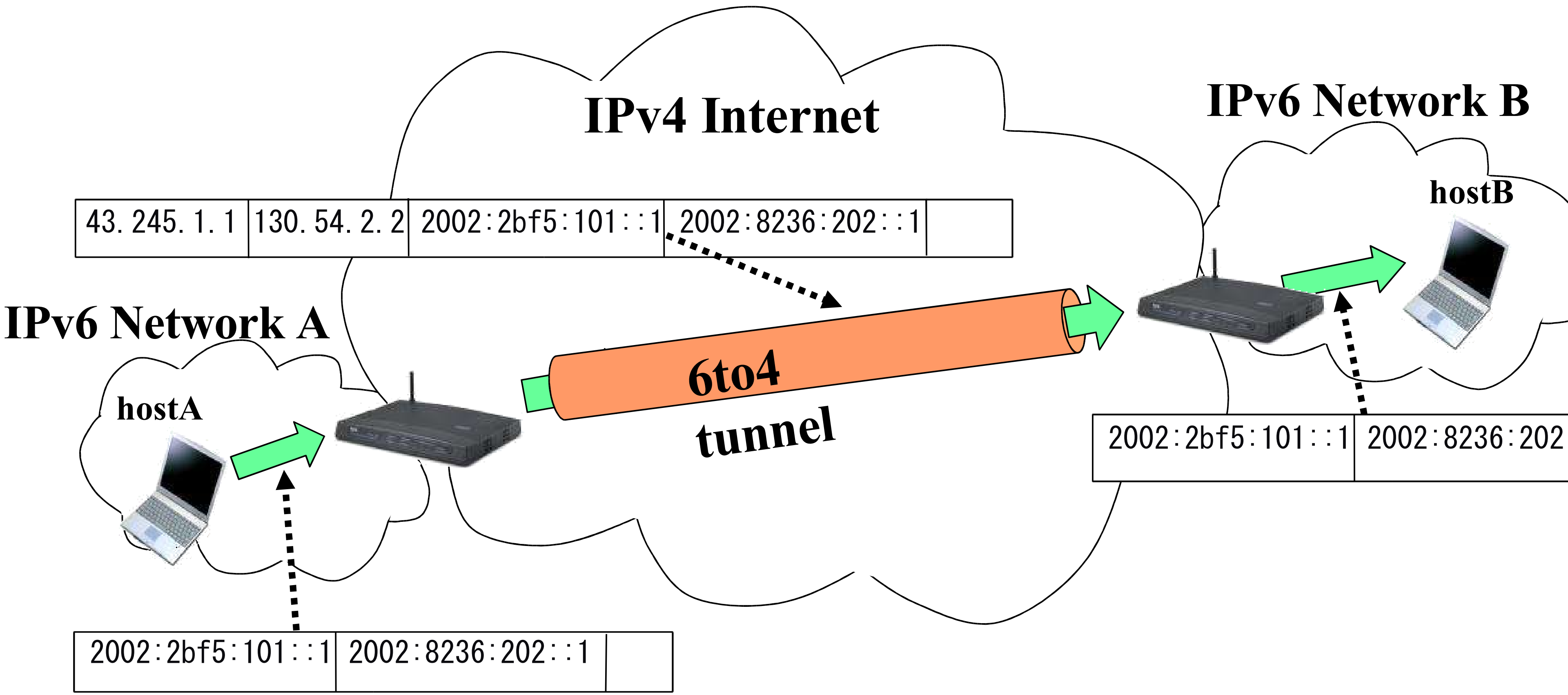
- **Functions for VPN is embended to Home Residential Gateway (HomeRG)**
  - Here, LIN6 is a mobility protocol (instead of MIPv6)
  - MIAKO.Net 4 IMPO



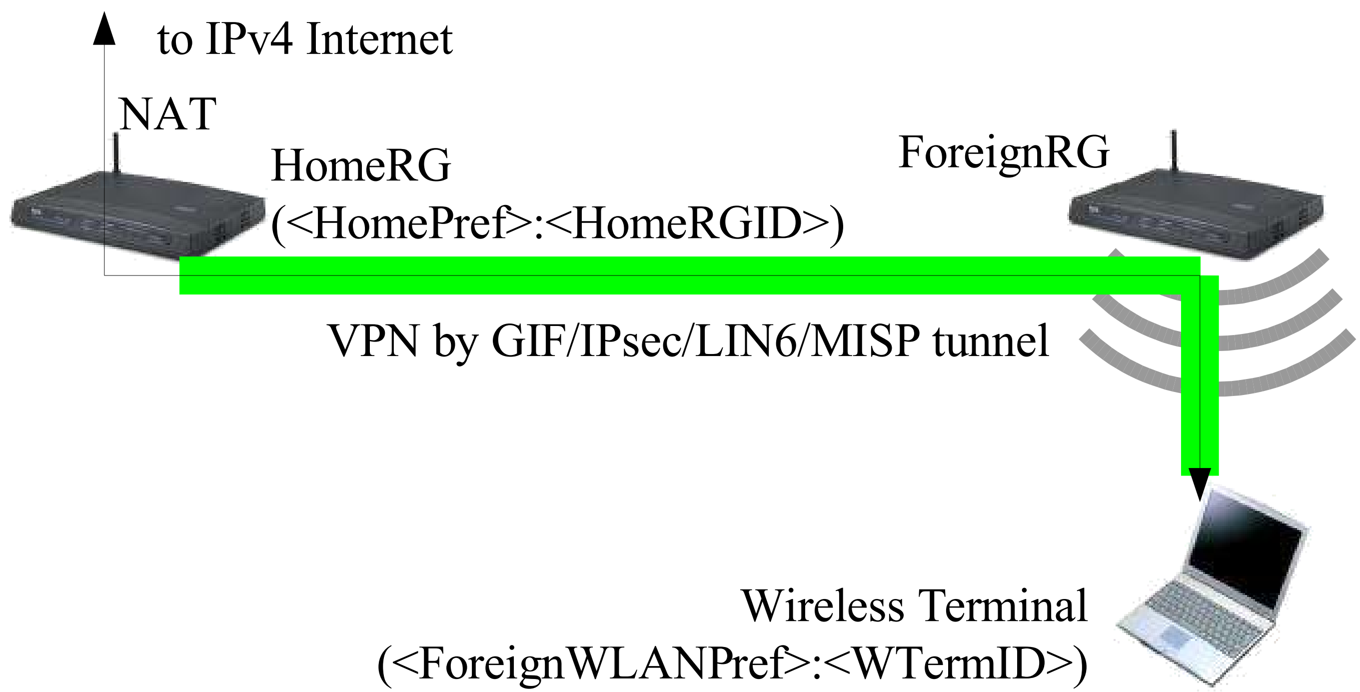
6to4 for interchanging IPv6 packets between HomeRG's



6to4 for interchanging IPv6 packets between HomeRG's (2)

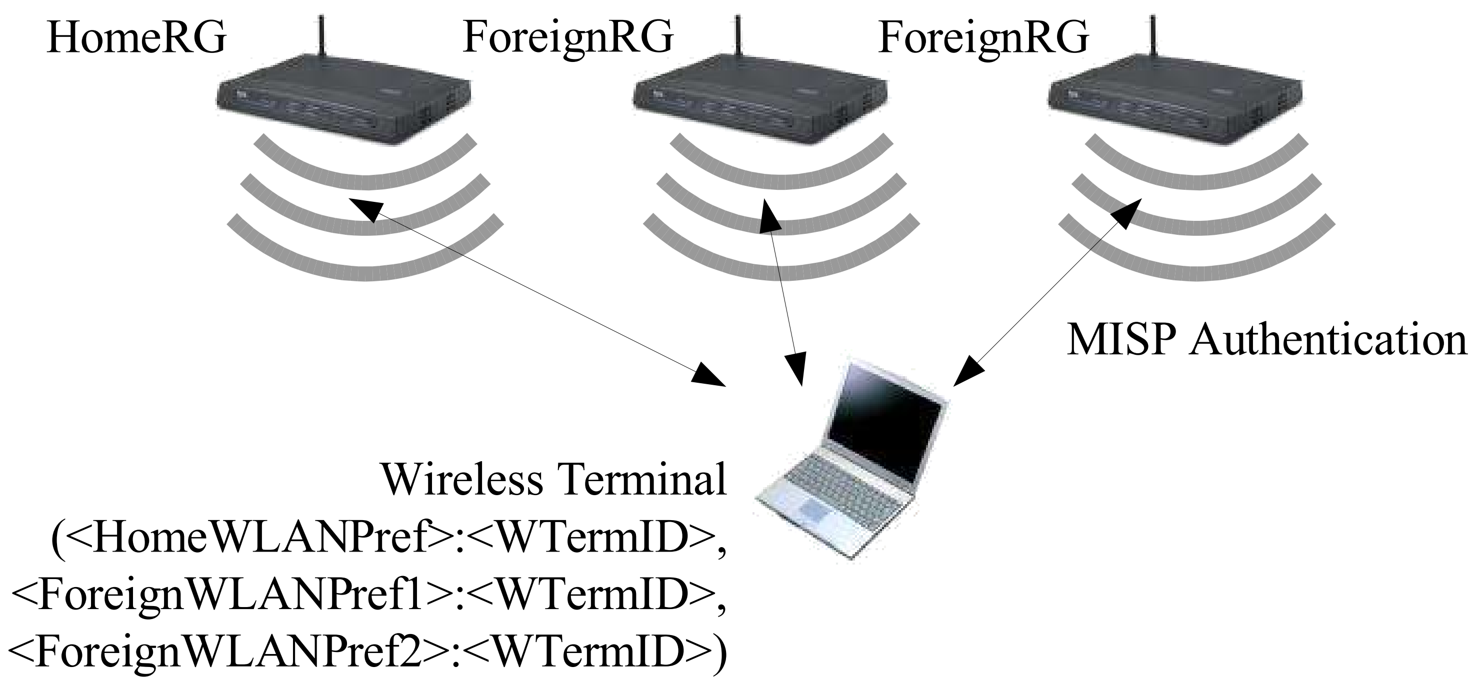


IPv4 connection over IPv6 VPN

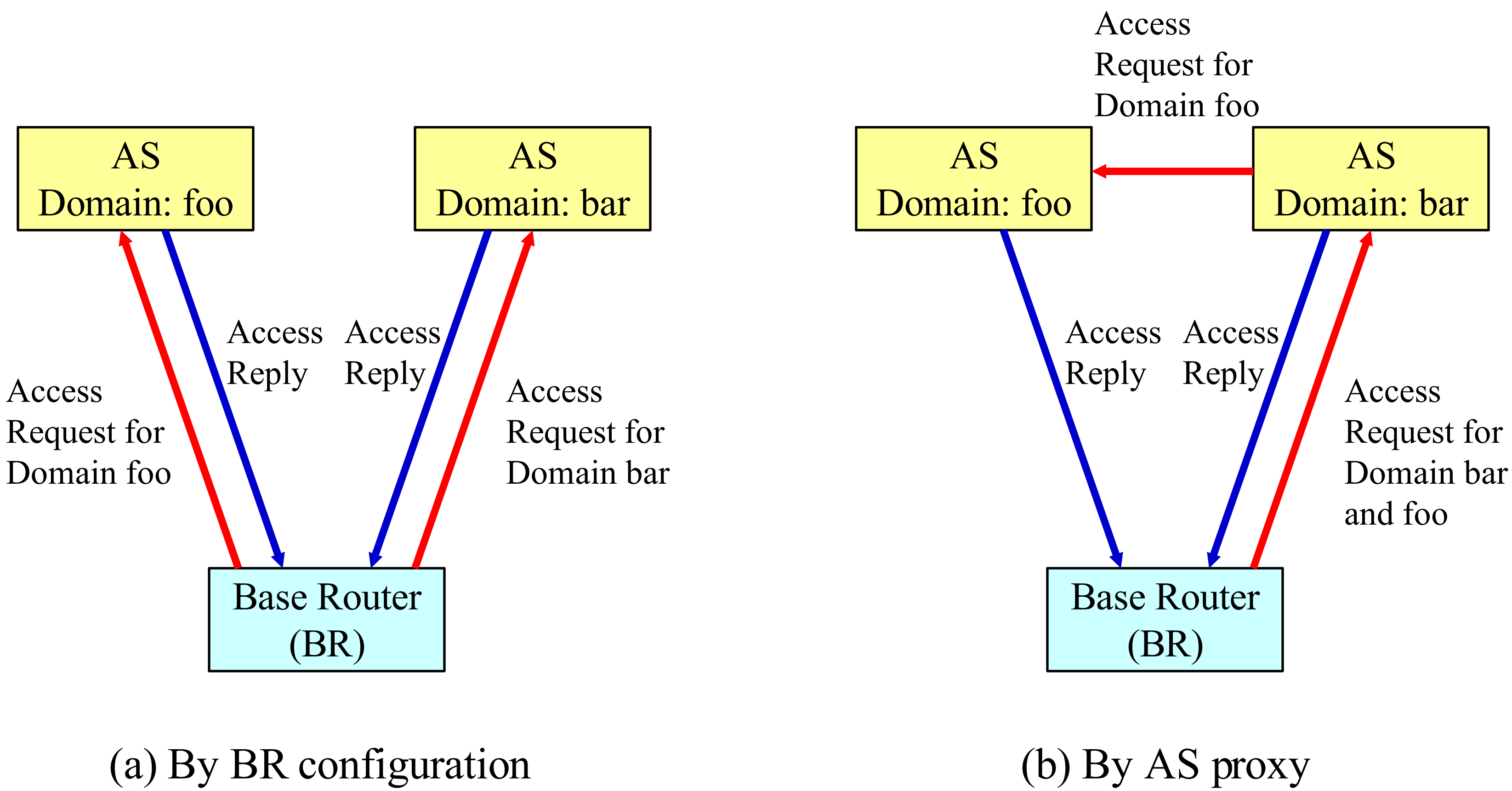


Advantages of MISP for VPN

- **Provides simultaneous access to multiple BR's (base routers, access points)**
- **Provides fast authentication**
- **Provides fast handover**



Multiple Service Providers Support



Questions and Comments?