

Eduroam-JP Update

Jan. 25, 2007

Tohoku University, JAPAN

Tetsuo Imai

Contents



- Introduction of the eduroam to Japan
- Issues in conventional Wi-Fi roaming and VPN-only policy
- R&D of UPKI Wi-Fi roaming infrastructure
- Summary

Introduction of the eduroam to Japan

What is eduroam?

- Global roaming infrastructure developed by TERENA Taskforce on Mobility in Europe (<http://www.eduroam.org>)
- Method of roaming that spreads in Europe and in some Asia-Pacific countries. (de facto standard)
- Based on IEEE802.1X and hierarchical RADIUS server tree.

Cyber Science Infrastructure (CSI)

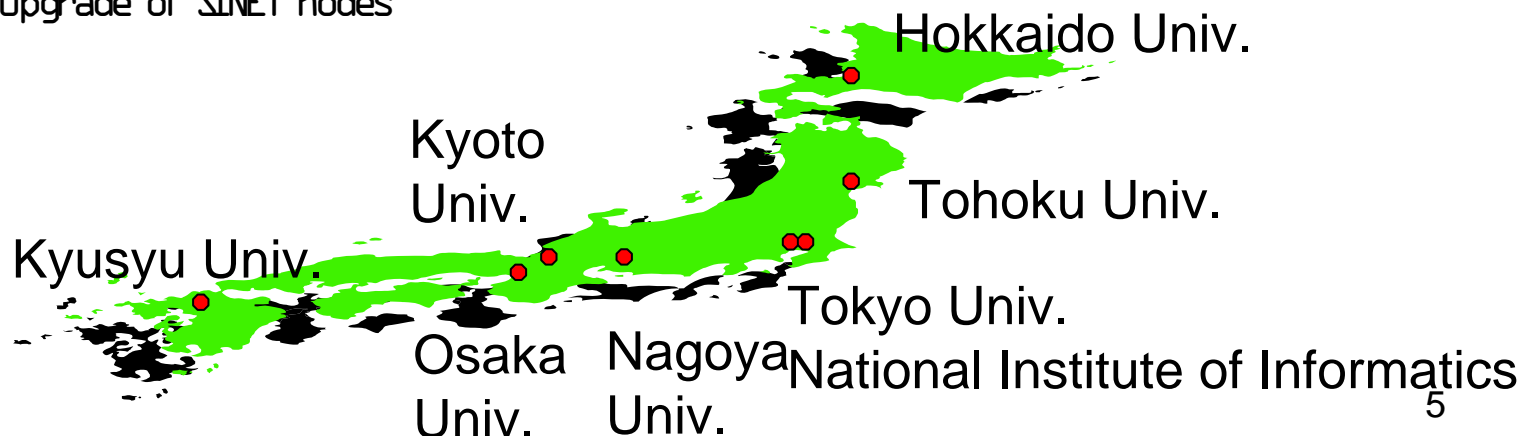
We have been working on campus ubiquitous network with the UPKI (University PKI) which is an authentication infrastructure between Universities.

- UPKI for collaboration between universities

The important infrastructure for safely services.

NII and Information Infrastructure center of seven universities collaborate for research and development.

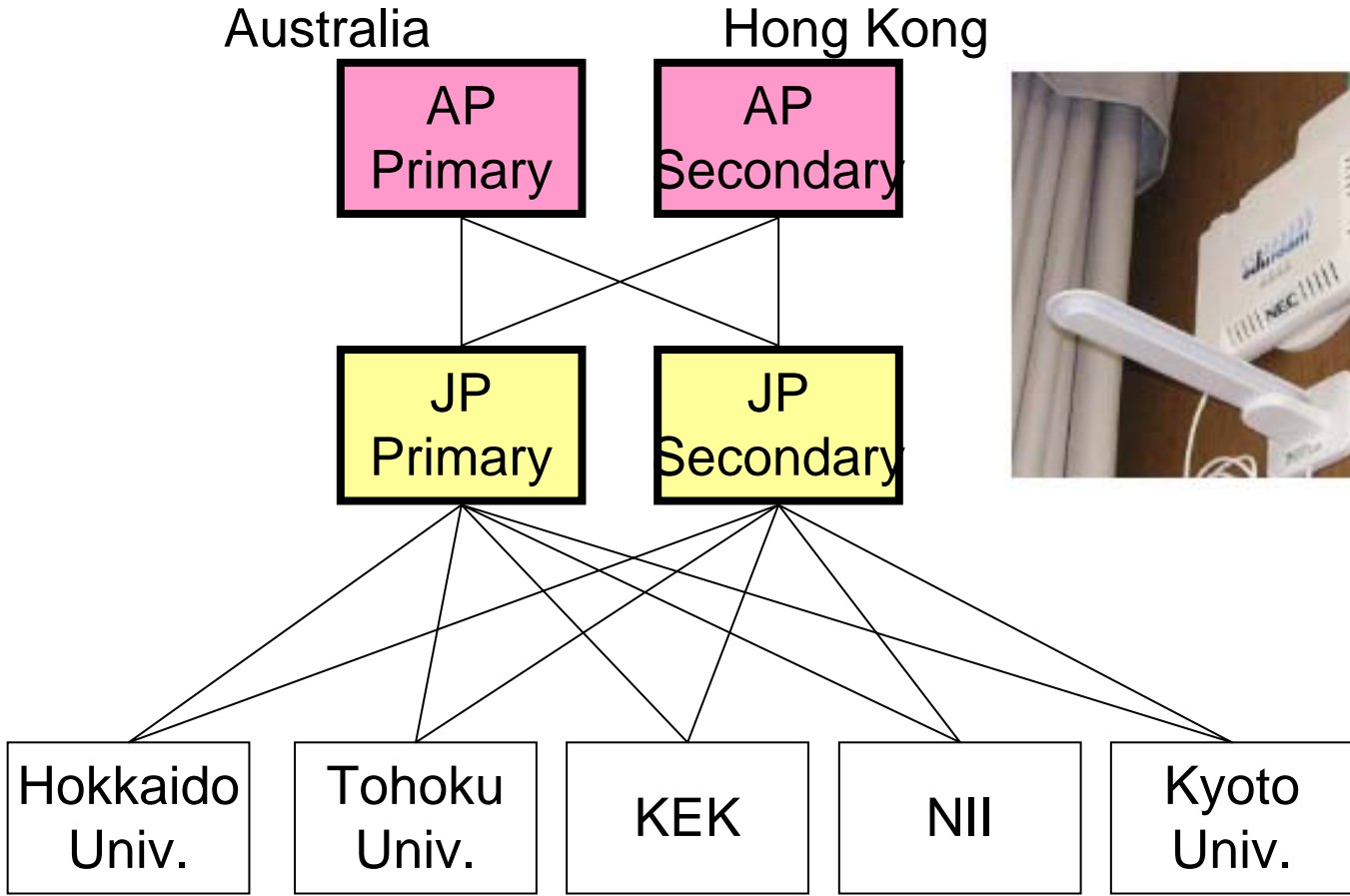
- Maintenance of authentication infrastructure for campus ubiquitous network
- Maintenance of grid environment
- Upgrade of SINET nodes



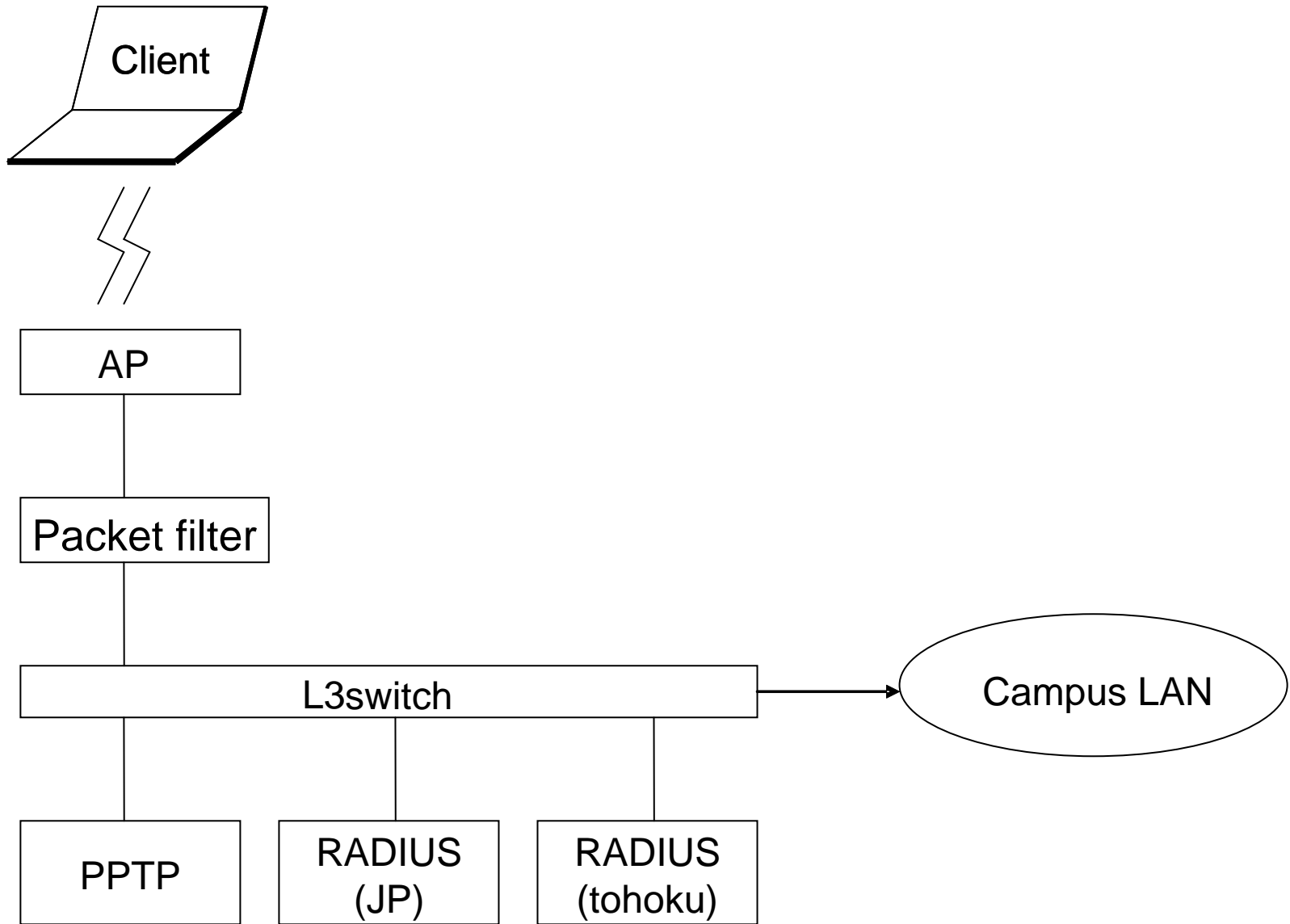
Joining eduroam

- Aug. 31, 2006. Early Introduction by Tohoku Univ. Information Center
- Sep. 28, 2006. eduroam.jp open
- In Dec., Hokkaido Univ. , Kyoto Univ. , National Institute of Informatics (NII), High Energy Accelerator Research Organization (KEK) have joined to the eduroam.

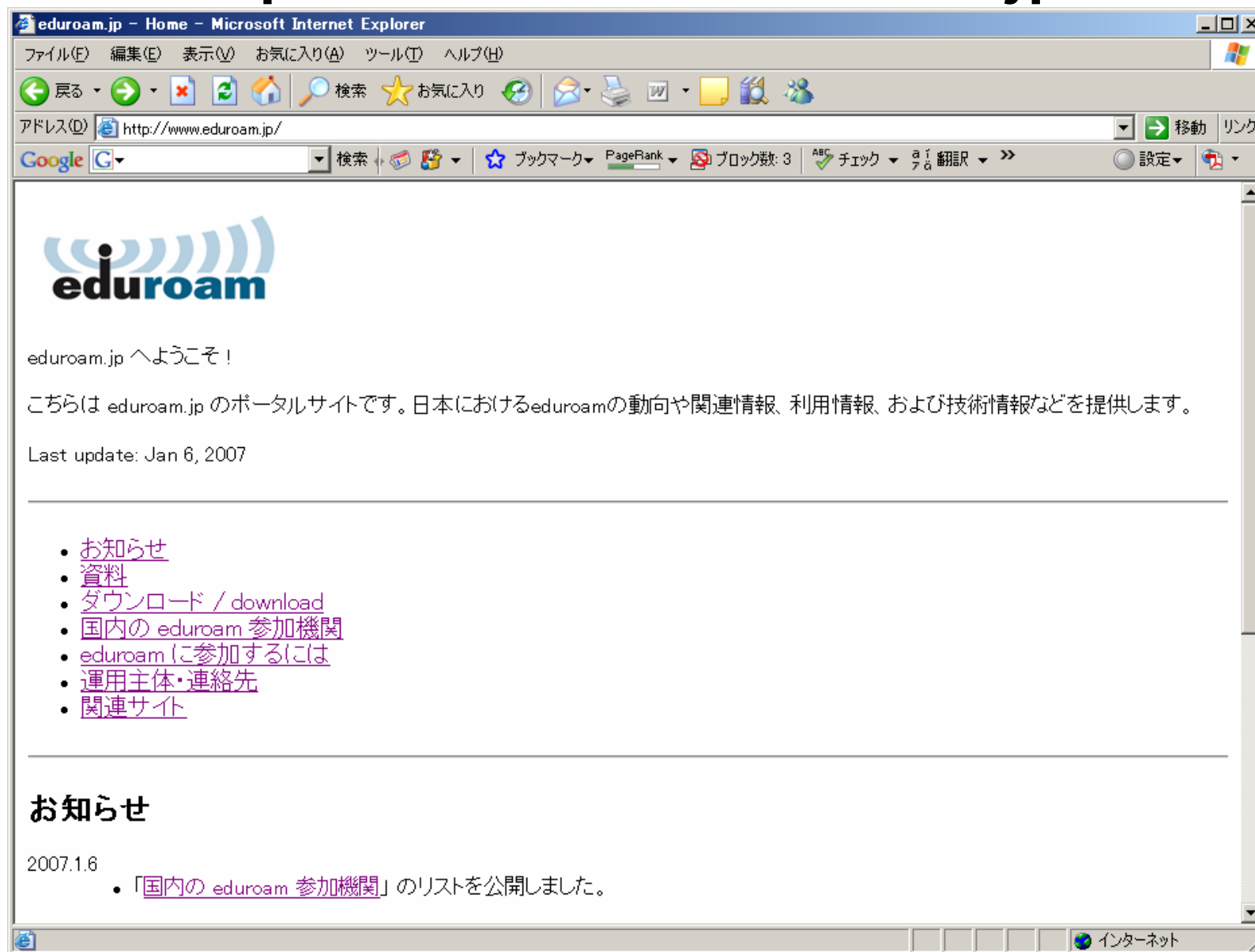
eduroam JP network



Network at Tohoku Univ.



http://www.eduroam.jp/



The screenshot shows a Microsoft Internet Explorer browser window with the address bar set to <http://www.eduroam.jp/>. The page content includes the eduroam logo, a welcome message, a description of the portal site, the last update date (Jan 6, 2007), and a list of navigation links. The status bar at the bottom indicates the connection is to the Internet.


eduroam.jp - Home - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 進む 検索 お気に入り

アドレス(ⓐ) <http://www.eduroam.jp/> 移動 リンク

Google G 検索 ブックマーク PageRank ブロック数: 3 チェック 翻訳



eduroam.jp へようこそ！

こちらは eduroam.jp のポータルサイトです。日本におけるeduroamの動向や関連情報、利用情報、および技術情報などを提供します。

Last update: Jan 6, 2007

- [お知らせ](#)
- [資料](#)
- [ダウンロード / download](#)
- [国内の eduroam 参加機関](#)
- [eduroam に参加するには](#)
- [運用主体・連絡先](#)
- [関連サイト](#)

お知らせ

2007.1.6

- 「[国内の eduroam 参加機関](#)」のリストを公開しました。

インターネット

eduroam.jp participants list by XML

eduroam.jp - Participants - Microsoft Internet Explorer

アドレス(D) http://www.eduroam.jp/participants/siteinfo.xml

Google G

eduroam.jp 参加機関 / Participants

Institution 機関	Department 部所	Site 場所	Prefecture 都道府県	Status 状況	Authn Used 認証方式	Access Granted 許可されたアクセス	Detailed site 詳細サイト
National Institute of Informatics 国立情報学研究所		Chiyoda-ku 千代田区	Tokyo 東京都	Deployed	802.1x ?	VPN	
Hokkaido University 北海道大学		Sapporo 札幌市	Hokkaido 北海道	Development	802.1x ?	?	
Tohoku University 東北大学		Sendai 仙台市	Miyagi 宮城県	Deployed	802.1x TKIP PEAP	VPN	
High Energy Accelerator Research Organization 高エネルギー加速器研究機構		Tsukuba つくば市	Ibaraki 茨城県	Federated	802.1x ?	?	
Kyoto University 京都大学		Kyoto 京都市	Kyoto 京都府	Federated	802.1x ?	eduroam_standard	
Kyushu University 九州大学		Fukuoka 福岡市	Fukuoka 福岡県	Development	802.1x ?	?	

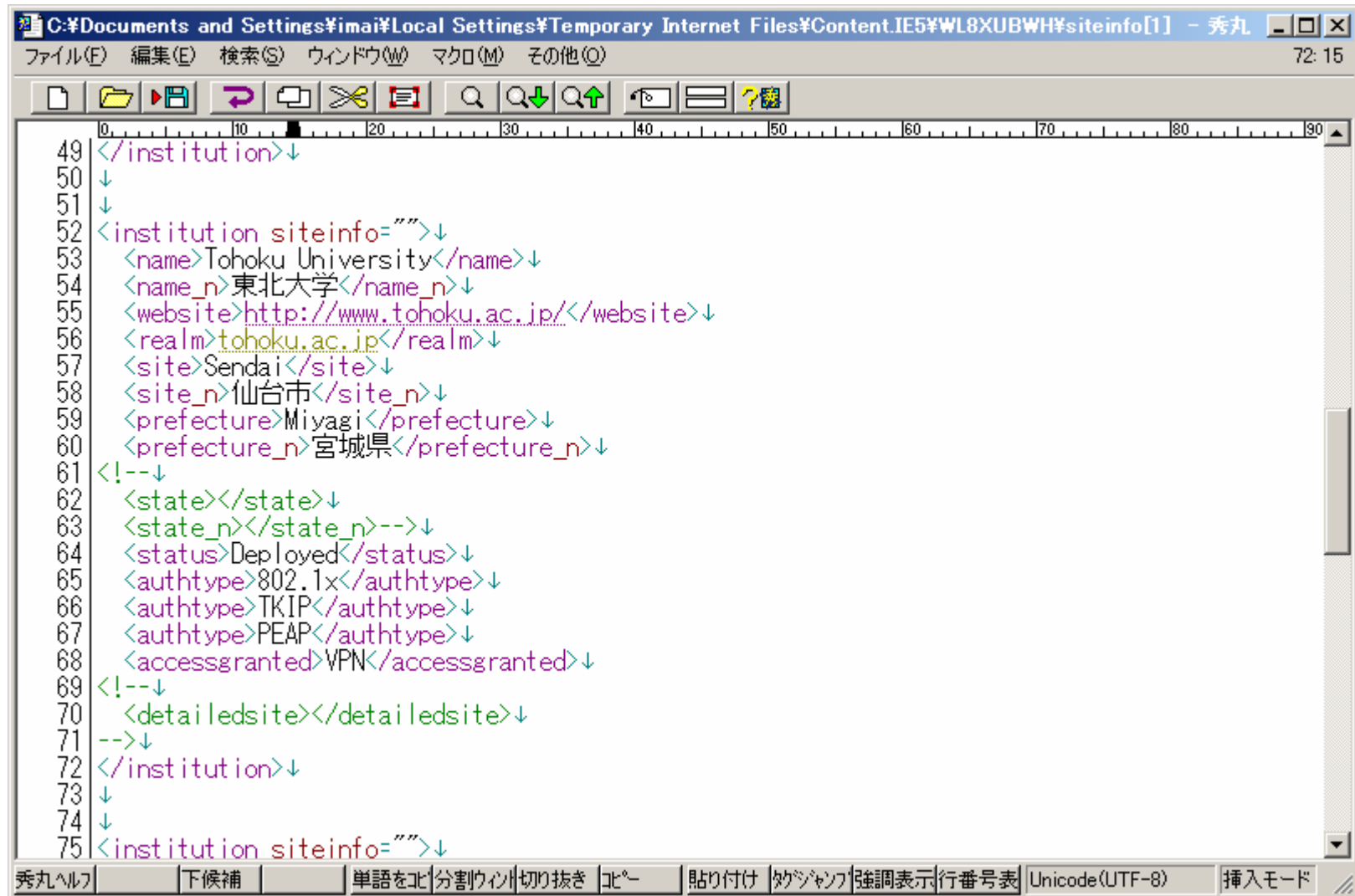
Status key

- Deployed: Site is federated to the eduroam system and wireless deployed.
- Federated: Site is linked to the eduroam system but wireless deployment is still under development or partially deployed.
- Development: Site is under development of eduroam system.
- Consideration: Site is under consideration for deployment.

Key of Access granted

インターネット

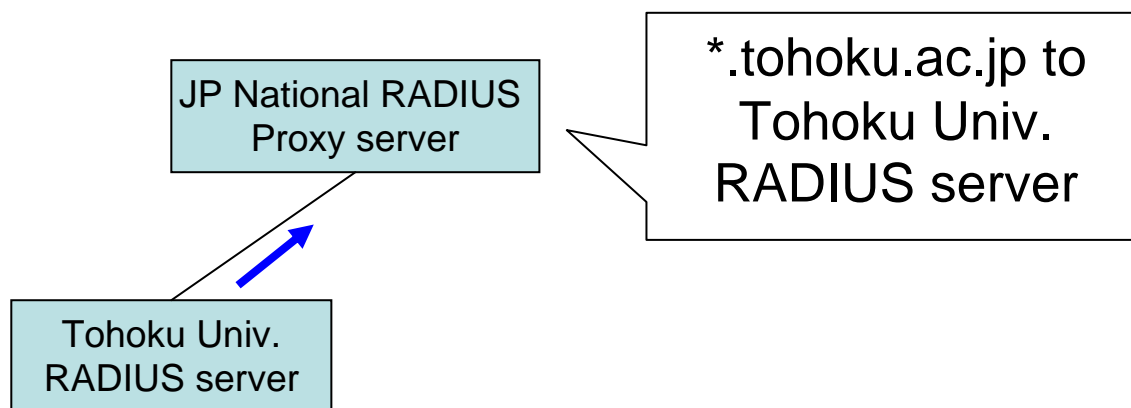
XML document



```
49 </institution>↓
50 ↓
51 ↓
52 <institution siteinfo="">↓
53   <name>Tohoku University</name>↓
54   <name_n>東北大学</name_n>↓
55   <website>http://www.tohoku.ac.jp/</website>↓
56   <realm>tohoku.ac.jp</realm>↓
57   <site>Sendai</site>↓
58   <site_n>仙台市</site_n>↓
59   <prefecture>Miyagi</prefecture>↓
60   <prefecture_n>宮城県</prefecture_n>↓
61 <!--↓
62   <state></state>↓
63   <state_n></state_n>-->↓
64   <status>Deployed</status>↓
65   <authtype>802.1x</authtype>↓
66   <authtype>TKIP</authtype>↓
67   <authtype>PEAP</authtype>↓
68   <accessgranted>VPN</accessgranted>↓
69 <!--↓
70   <detailedsite></detailedsite>↓
71 -->↓
72 </institution>↓
73 ↓
74 ↓
75 <institution siteinfo="">↓
```

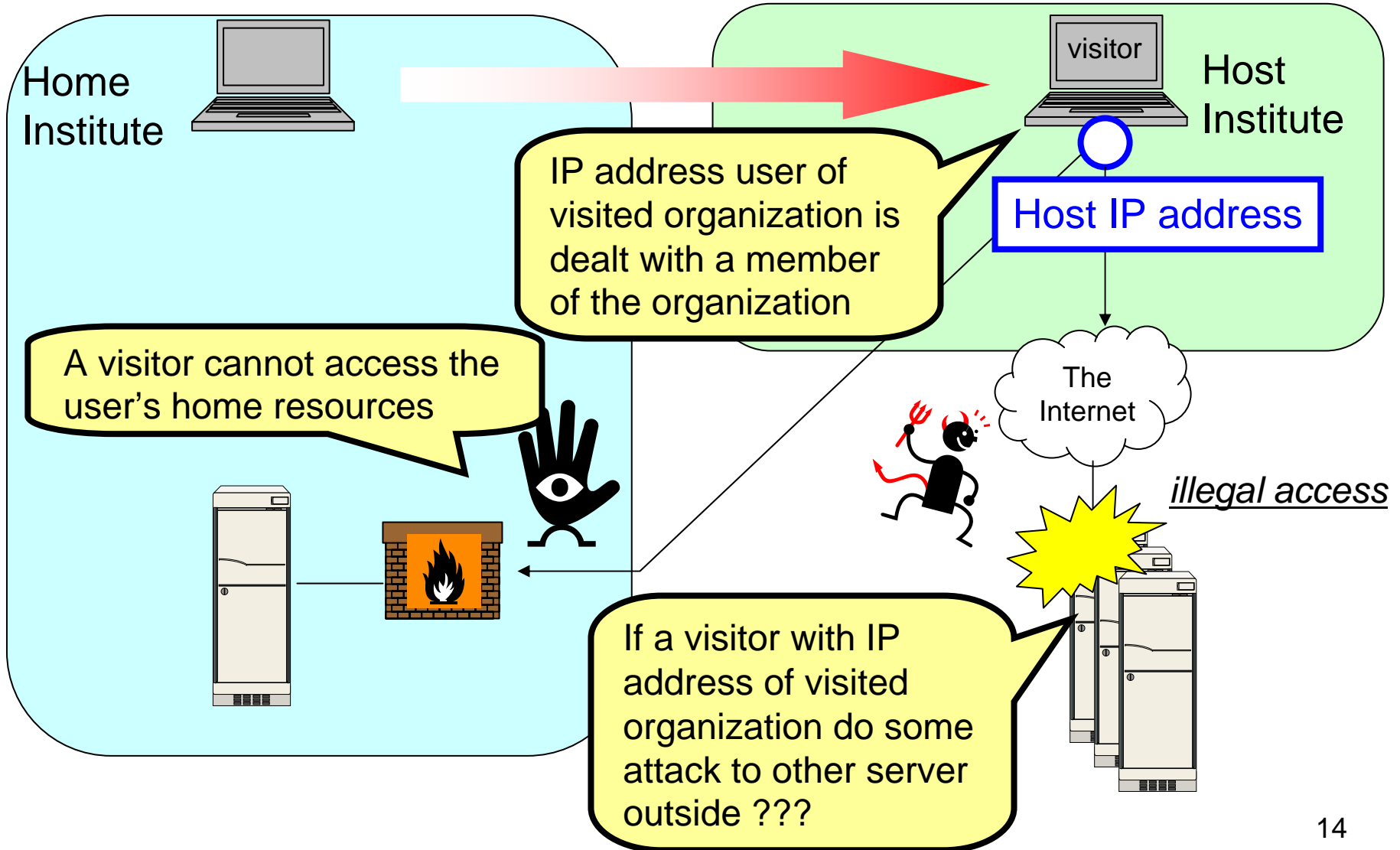
FreeRadius patch

- A patch that enable proxying with regular expression on FreeRADIUS



Issues in conventional Wi-Fi roaming and VPN-only policy

The Problem about traceability



Traceability : case study 1

Though university A is not subscribing to electronic journal X, another university B is subscribing. A student at univ. A goes to univ. B so he/she can download journal X using the Wi-Fi roaming. Since the student downloaded too many articles at once, the publisher thought it was a violation of the subscription condition and sent a complaint to univ. B.

In University B, NW manager have to analyze the roaming logs, and with telling to University A, have to look for the user.

Huge human cost is spent.

Even between departments in a university, such a user tracking is difficult. It is very difficult between universities. It is also very difficult between countries, all the more.

Traceability : case study 2

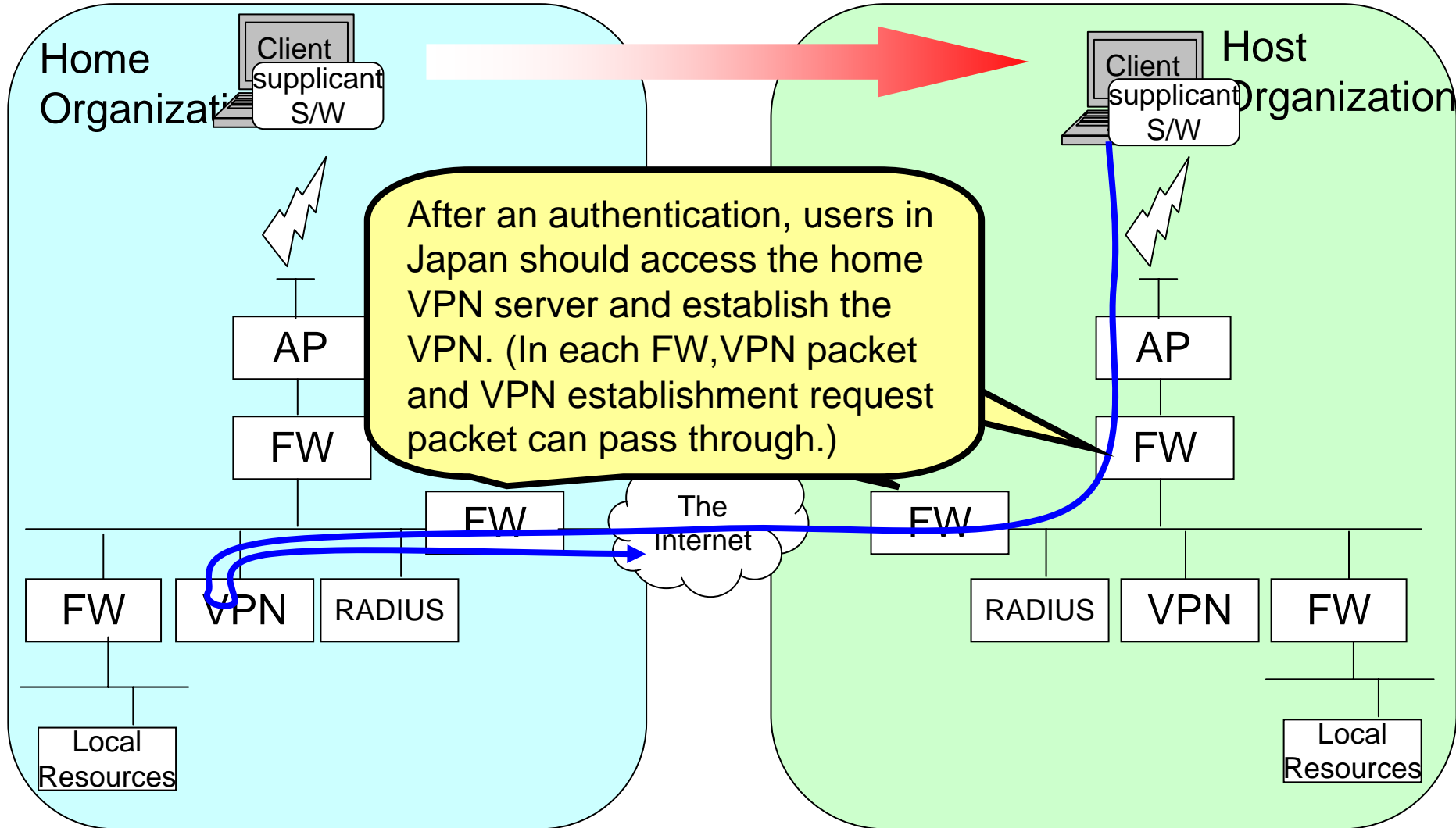
Some resources such as local web servers in univ. B are protected by an address-based access restriction. If people in univ.A visit univ. B, they can gain access to the resources using the Wi-Fi roaming system.

Though the manager of the web server looks the access logs, the outsider's access is not noticed easily because IP addresses inside the university are used.



Use their home IP addresses

VPN-only policy for Japan

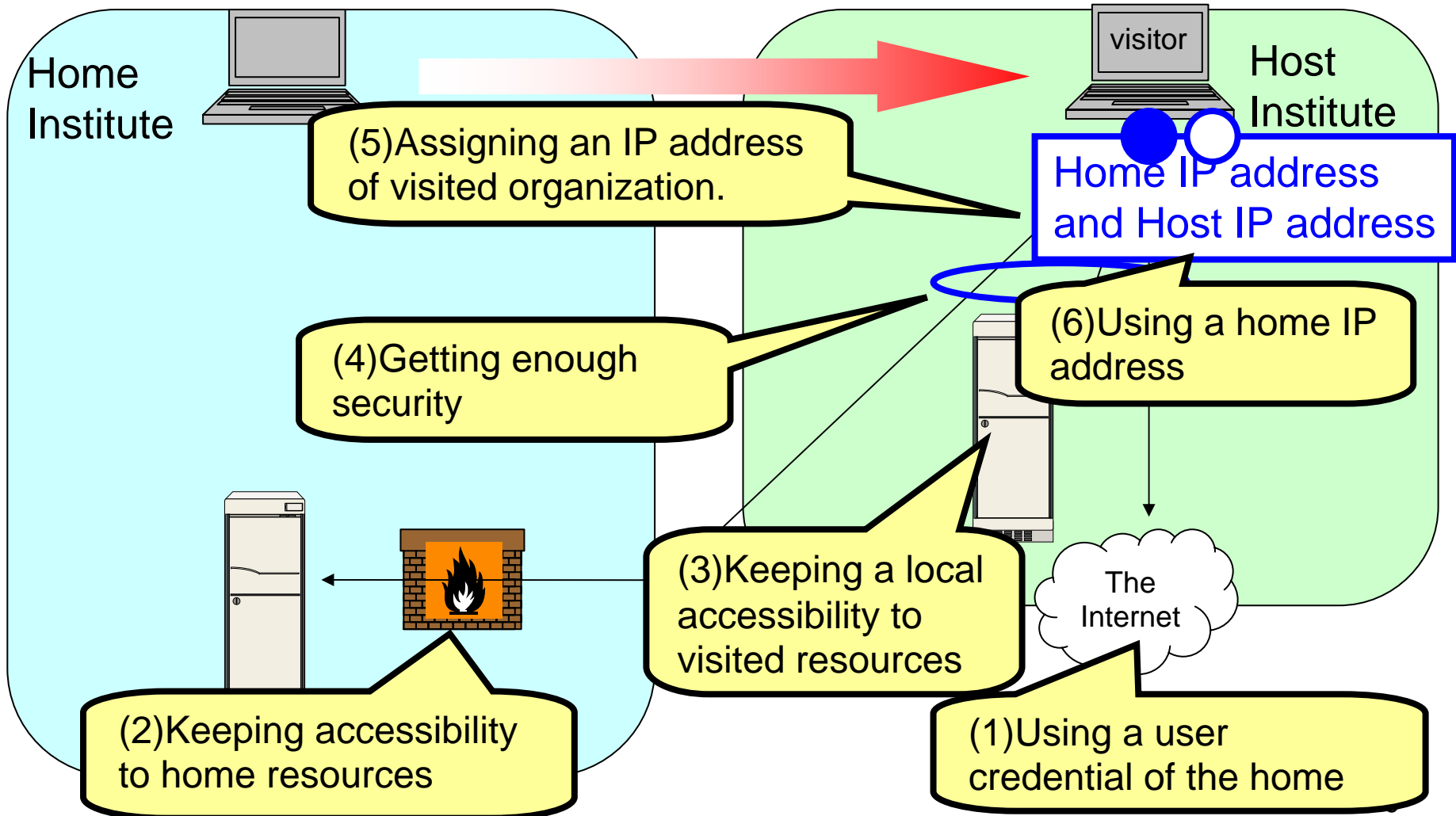


Available protocols

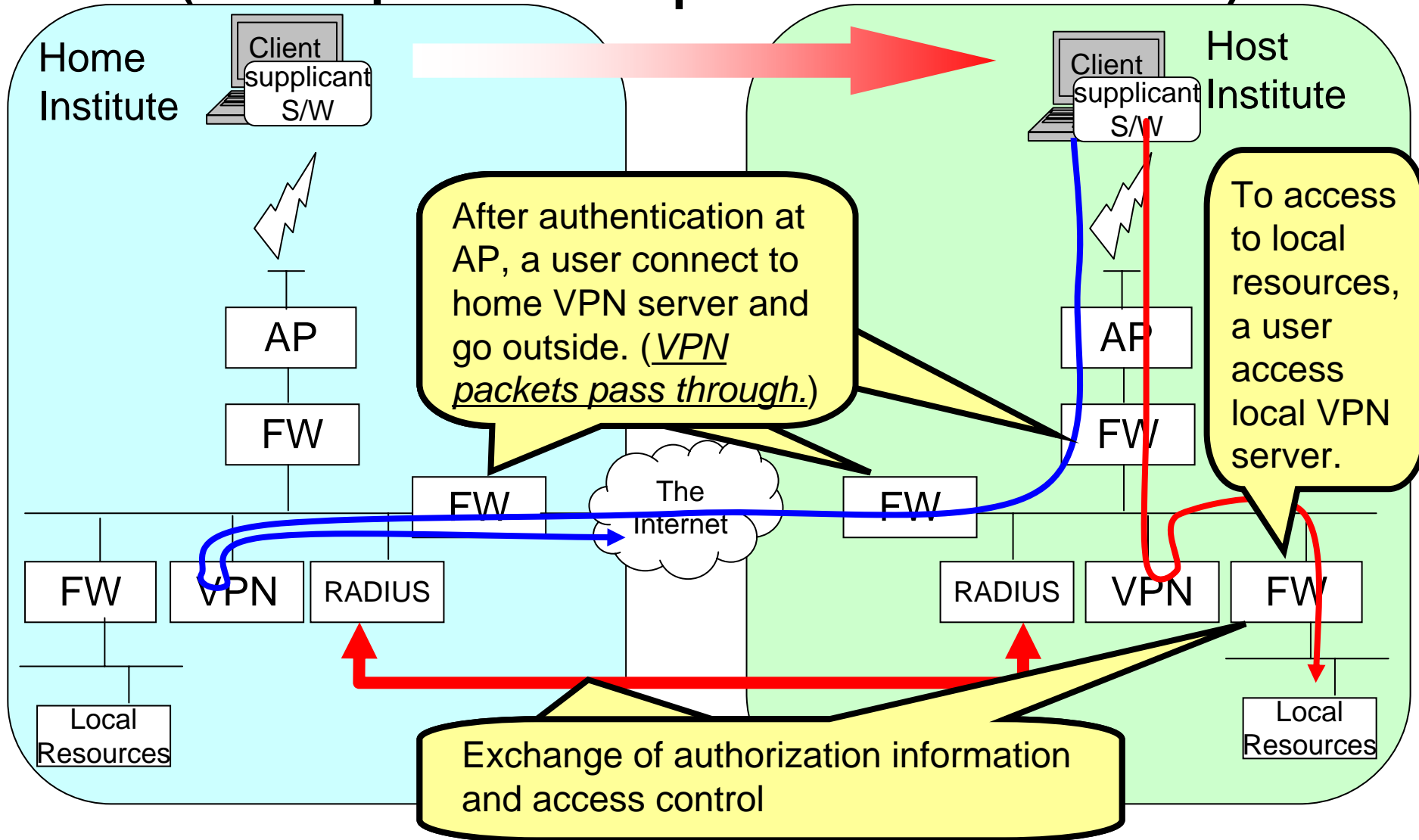
- RADIUS(UDP/1812)□(UDP/1813)□
- Standard IPSec(ESP(50)□(AH(51)□(IKE(UDP/500))□
- Cisco IPSec(TCP/10000)
- OpenVPN(UDP/1194)□
- PPTP(GRE(47)□(TCP/1723))□
- pop3(TCP/110)□
- pop3s(TCP/995)□
- imap4(TCP/143)□
- imaps(TCP/993)□
- ssmtp(TCP/465)□
- msa(TCP/587)□
- SSH(tcp/22)

R&D of UPKI Wi-Fi roaming infrastructure

The requirements of roaming system



Proposing method (Campus Ubiquitous Network)

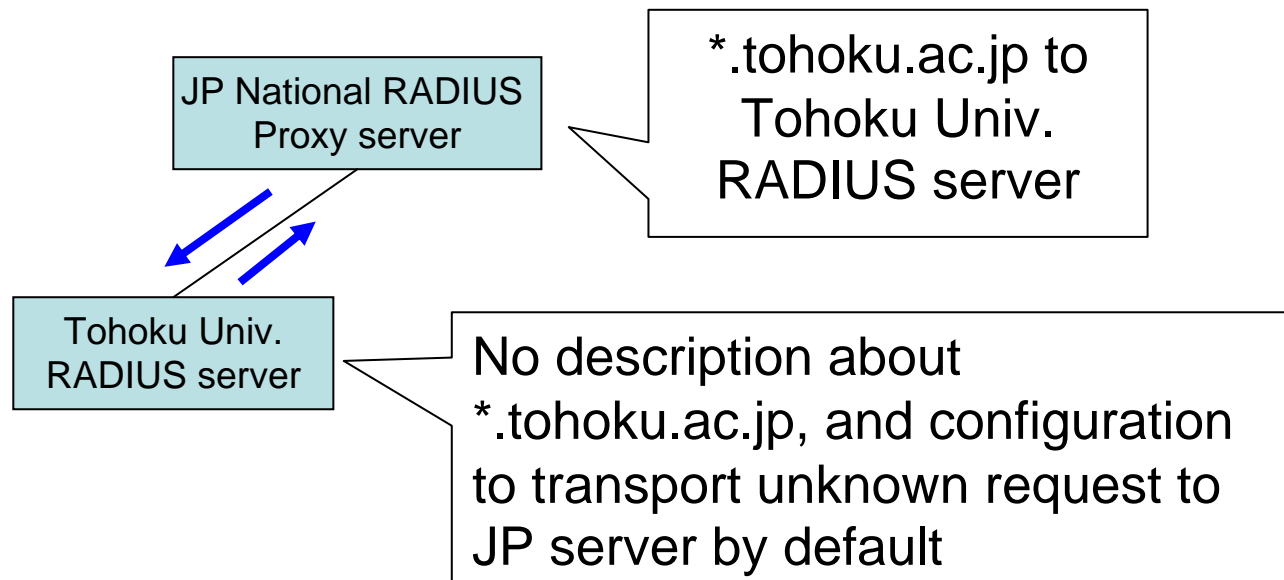


Summary

- Introduction of the eduroam to Japan
- Issues in conventional Wi-Fi roaming and VPN-only policy
- Proposing campus ubiquitous network (fundamental idea)

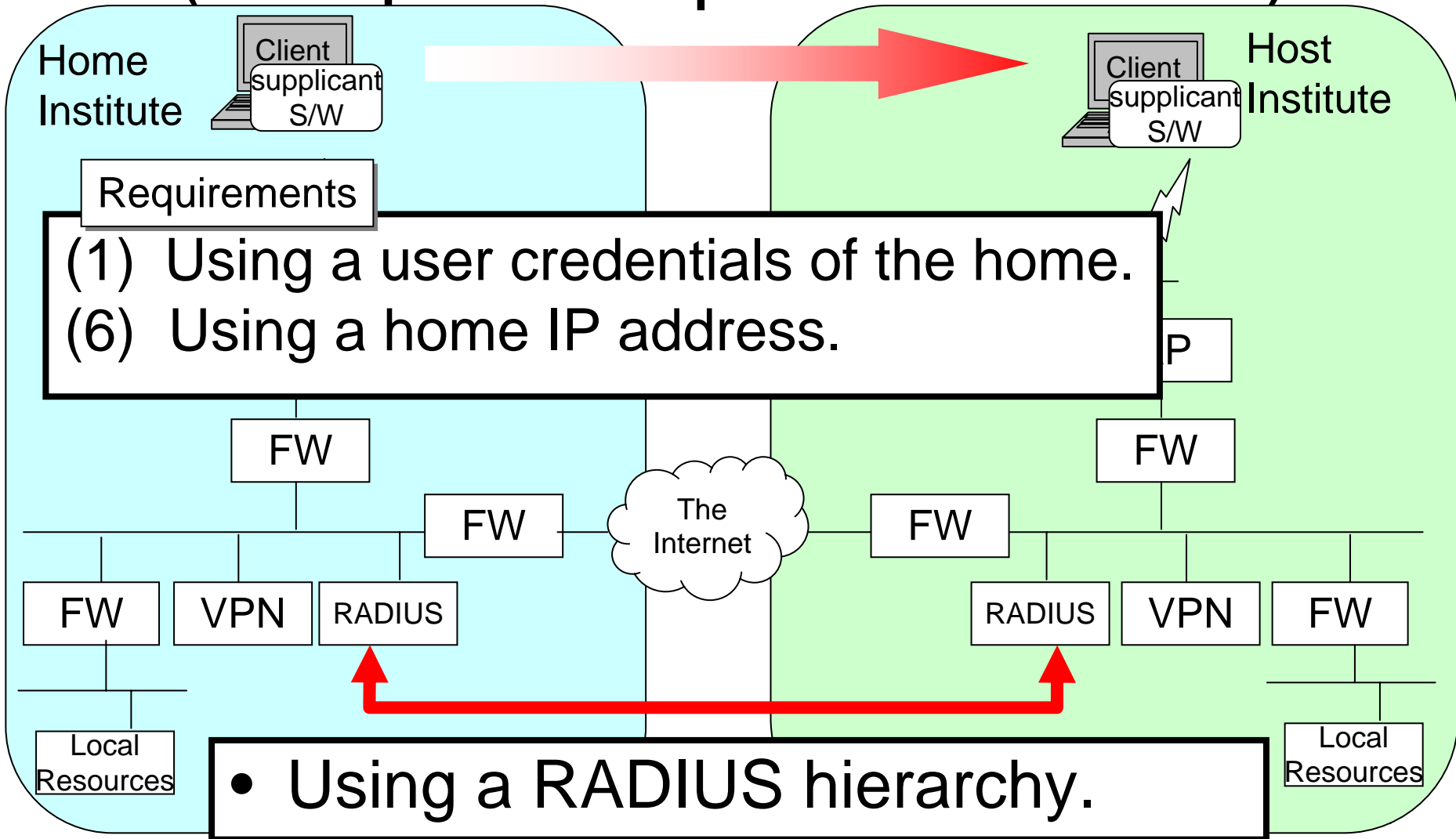
Attention of the configuration of the FreeRadius(avoidance of loops)

- By the RADIUS configuration of each organization, there is a possibility that the loop is generated between an each organization's server and the JP server.



□ Each organization must describe in proxy.conf that they process requests of their own domain

Proposing method (Campus Ubiquitous Network)

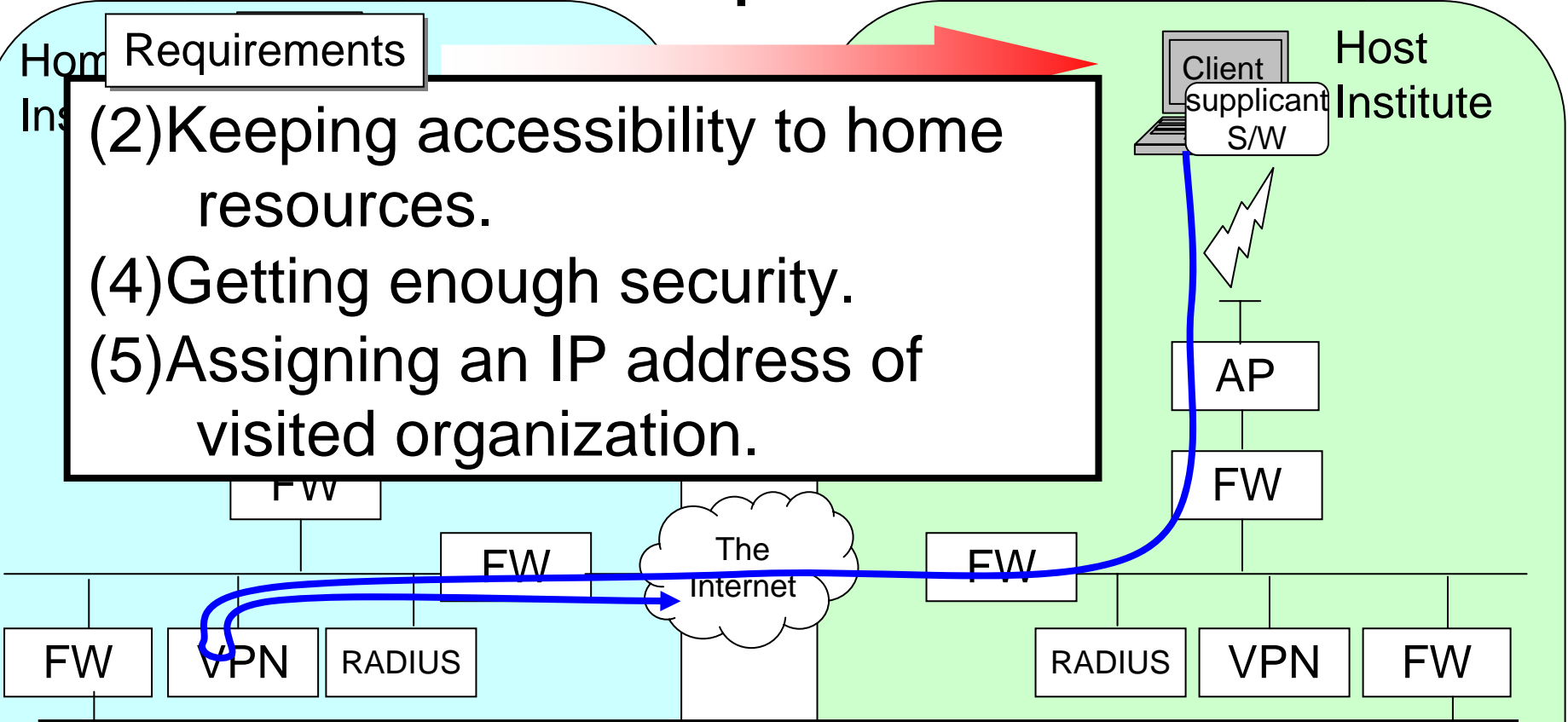


Proposing method (Campus Ubiquitous Network)

Home Requirements

- (2) Keeping accessibility to home resources.
- (4) Getting enough security.
- (5) Assigning an IP address of visited organization.

Host Institute
Client supplicant S/W



- Using a home VPN server and home IP address

Proposing method (Campus Ubiquitous Network)

