RouterBOARDとLTEデバイスによる

可搬型Hotspot2.0/Passpoint基地局

札幌学院大学　情報処理課　　原田寛之

How do you stay safe on public Wi-Fi while traveling?

Your University/Office/Home

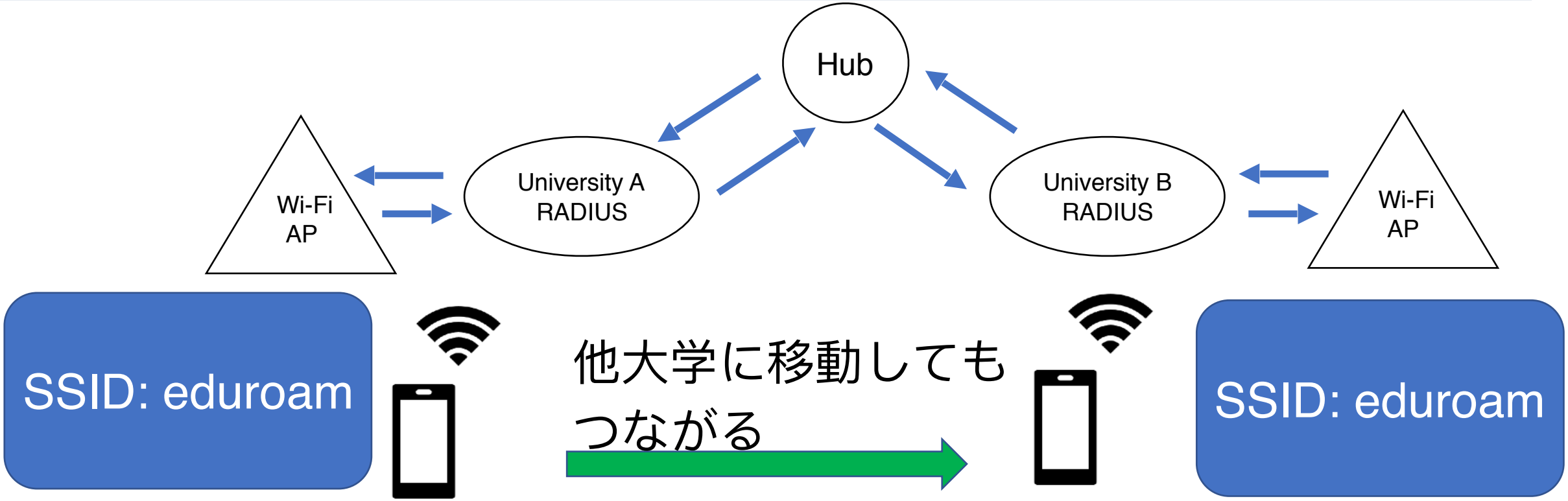
Public Wi-Fi

SSID? Encryption?
Username? Password?

802.1X authentication roaming （eduroamの場合）

- eduroam （大学等でのキャンパス無線LAN相互利用）加入機関で

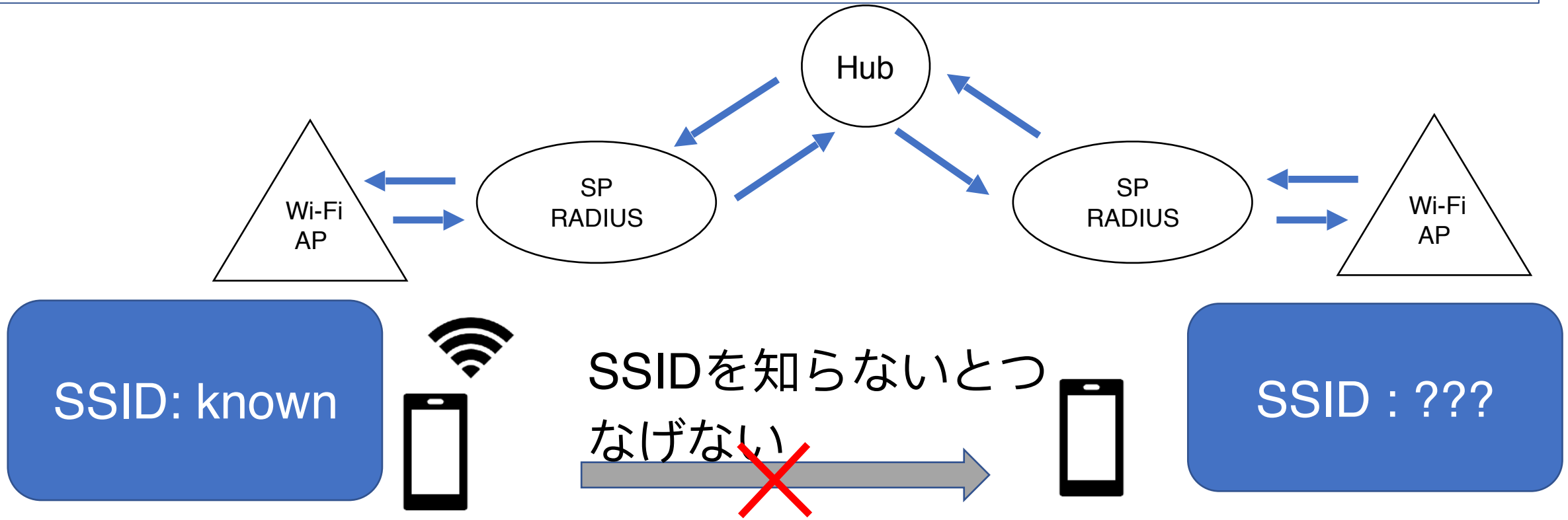
  は、共通の SSID: eduroam を吹いている



802.1X authentication roaming (SSIDが共通でない場合)

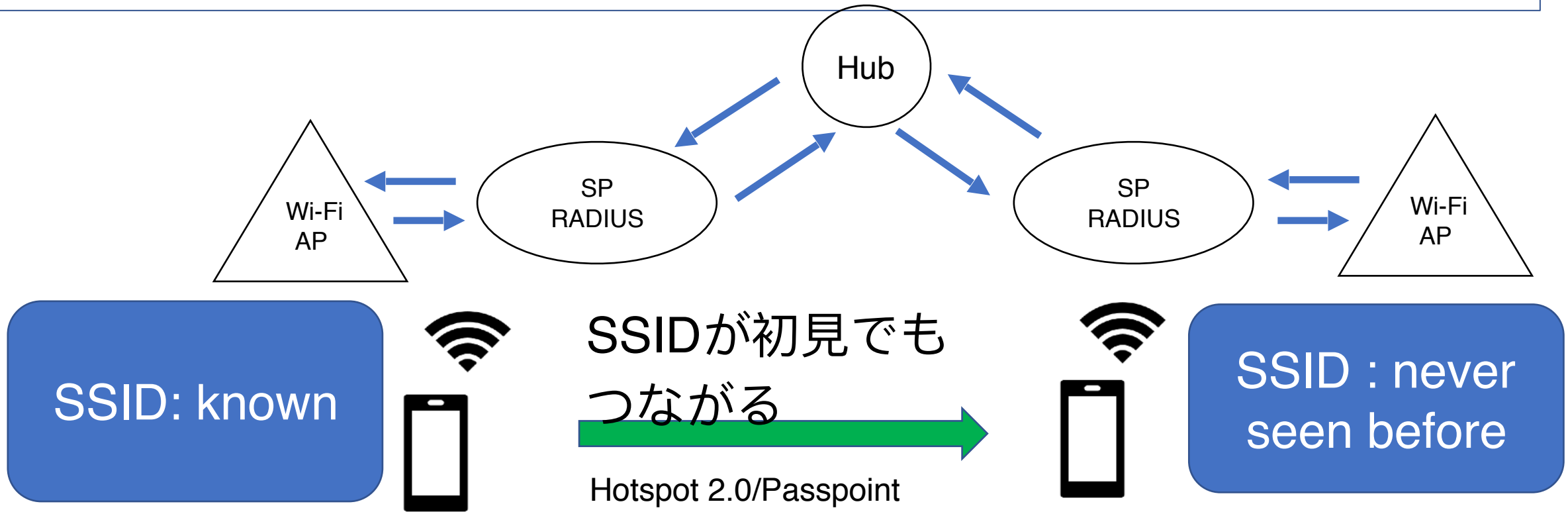
- ユーザは、街中のPublic Wi-Fiが自分のIDを発行した機関と

  認証ローミングされていてもSSIDがわからないと接続できない



802.1X authentication roaming and Hotspot 2.0 / Passpoint

- 初見のSSIDであってもAPと基地局が相互に接続可能か情報交換する
- 自組織と認証ローミングされている場合は接続を自動的に行う



Demo 1 (ユーザー端末上での Passpoint / Hotspot 2.0の挙動)

可搬型Passpoint/Hotspot 2.0
基地局ができるまで

Which AP supports Hotspot 2.0 /Passpoint ?

そもそも個人で検証するには情報が少なかった

Cisco Merakiでの検証からスタート

→ 気軽に検証するには高い

→ Hotspot 2.0はβ機能で一般公開されていない

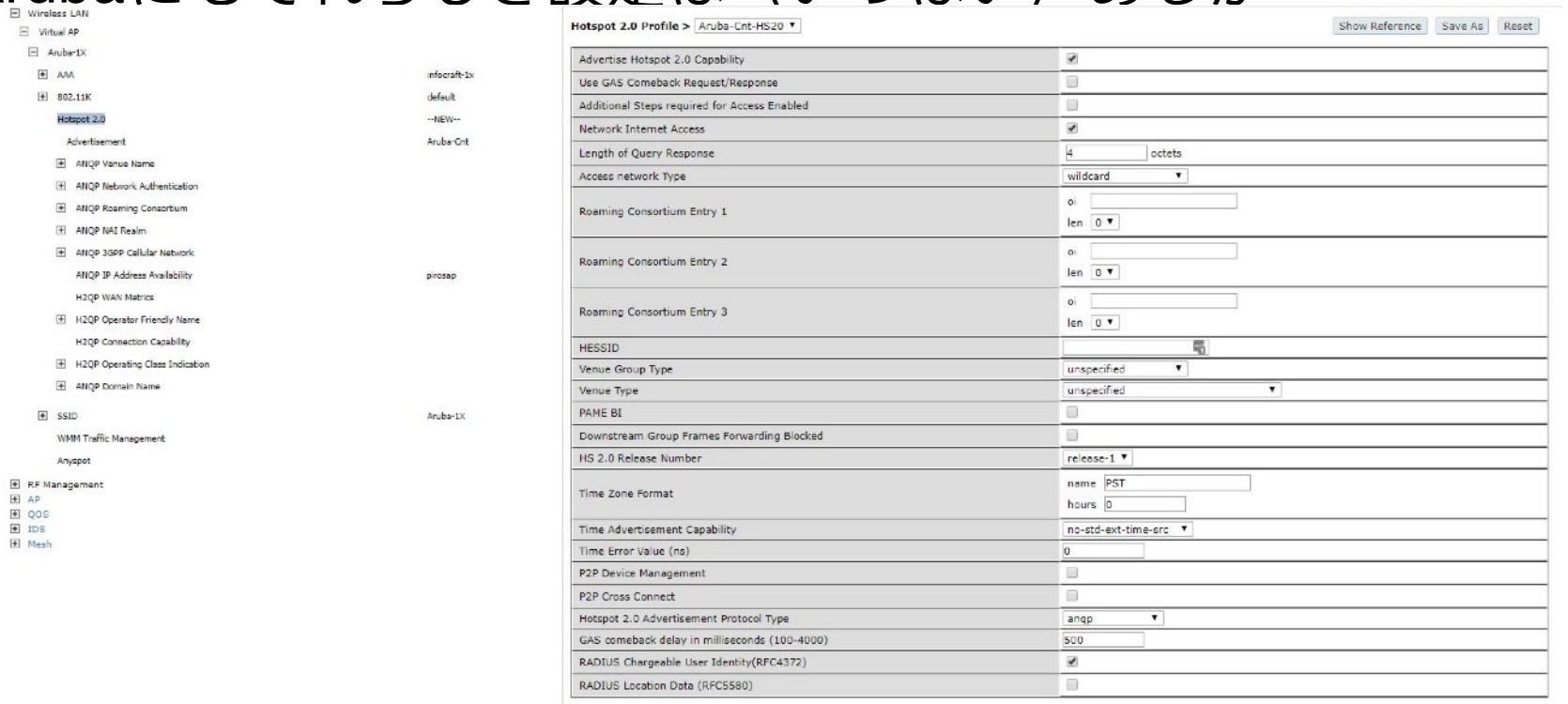
→ そもそも設定値の意味がよくわからない

→ コントローラ（クラウド）が必要で、単独では動作しない

→ もう少しお手軽なAPが欲しい（技適付きの）

Which AP supports Hotspot 2.0 /Passpoint ?

自宅のArubaにもそれらしき設定は（いっぱい）あるが



なんじゃこれ状態

Which AP supports Hotspot 2.0 /Passpoint ?

そんな時に見つけた
インドネシアのRofiq Fauziさんの
プレゼン

“MikroTik Hotspot 2.0 / IEEE 802.11u“

MikroTik ??

MikroTik Hotspot 2.0 (IEEE 802.11u)

視聴回数 1,433 回

MikroTik
2016/10/24 に公開

MikroTik Hotspot 2.0 (IEEE 802.11u), Rofiq Fauzi (ID-Networkers, Indonesia). PDF:
http://mum.mikrotik.com/presentations....

もっと見る

https://www.youtube.com/watch?v=My22bkfuVZo

MikroTikのAPで
技適を取っているものがあるか

AKIBA PC Hotline! 〉 PC周辺機器 〉 無線LAN (Wi-Fi) 〉 その他

ニュース

RouterOS搭載の11ac無線LANルーター「hAP AC」が販売中、国内向け

ラトビアのMikroTik製

AKIBA PC Hotline!編集部　2016年11月16日 12:05

ツイート リスト　いいね！ 136　シェア　B! 13　Pocket 47

ラトビアMikroTikの11ac無線LANルーターが登場、「hAP AC（RB962UiGS-5HacT2HnT）」がヴィゴネットラボ 秋葉原店で販売中だ。同店による1年間保証が付属し、また技適マークは取得済みとのこと。店頭価格は税込29,700円。

あった

MikroTik hAP acでHotspot 2.0

できた

MikroTik hAP acでHotspot 2.0

サポートが熱い

100% CPU usage with Hotspot 2.0 and disconnect wireless client

+ Post Reply | Search this topic...

pirosap
just joined

Topic Author
Posts: 2
Joined: Sun Apr 23, 2017 5:37 pm

Sun Apr 23, 2017 6:10 pm #1

Hi. I'm developing Hotspot 2.0 wireless service with hAP ac (RB962UiGS-5HacT2HnT).
The RouterOS version is 6.38.5 (stable), and I'm testing with iPhone 6S (iOS 10.3.1).
The radius server is freeradius 3.0.10 and authentication is PEAP-MS-CHAPv2.

I could connect hAP ac with iOS that installed my hotspot2.0 .mobileconfig profile. It works with Cisco Meraki Hotspot 2.0.
But hAP ac disconnect the wireless connection after 10-30 minitue.

I found when hAP disconnect the client, its reached 100% CPU usage.
When I got this situation, I can reboot hAP ac from CLI, and set interworking-profile again, the connection back.
Otherwize the client can not reconnect without set interworking-profile again.

I din't have any problem without Hotspot 2.0 function, I mean if I didn't set the interworking-profile to wireless interface and connect with just 802.1x PEAP-MS-CHARv2, it is stable.

hAP acをPasspoint/Hotspot 2.0基地局にする

Wirelessインターフェースを802.1xのAPとして設定

> /interface wireless security-profiles add name=1X
> /interface wireless security-profiles set 1 mode=dynamic-keys authentication-types=wpa2-eap eap-methods=passthrough
> /radius set 0 service=wireless address=x.x.x.x secret=xxxxxx

Hotspot 2.0の設定としてinterworking-profileを設定

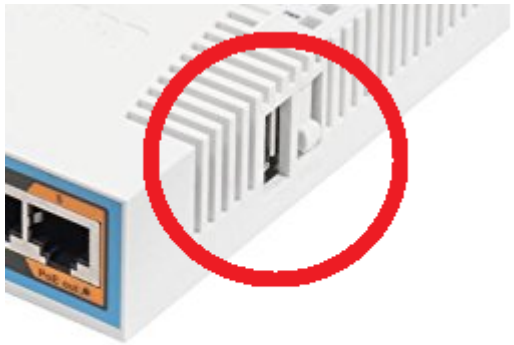
> /interface wireless interworking-profiles add name=pirosap
> /interface wireless interworking-profiles set 0 domain-names=ngh.pirosap.tech operator-names="NGH testbed by pirosap.tech”

上記を適用
> /interface wireless set 1 interworking-profile=pirosap

Hotspot 2.0/Passpointを広めたい

Hotspot 2.0基地局となったhAP acを使って
いろんな人に仕組みを見てほしい

しかし、出先に回線があるとは限らない



hAP acにはUSB接続の LTE/3Gドングルを接続できる

国内で技適取得済のLTEドングルは中々見つからなかった（3Gなら使えるものもあるが古い）

Model	備考	検証結果	検証日
AndroidのUSBテザリング	SO-01Gで検証	○　但しテザリングのためNATされる	-
L-03D(NTT Docomo)	LG	× /port usbで認識せず	2017/05/04
L-03F(NTT Docomo)	LG　※事前にPCでデータ通信専用モードに設定	× NDIS、PPP共に/port usbで認識せず	2017/05/04
WM320（SIMフリー）	富士ソフト	× /port usbで認識せず	2017/05/04
HX006ZT(Willcom)	ZTE MF633として認識 HX006ZT - ZTE Japan	○ Docomo SIMで3G接続確認。moperaであればppp-outにグローバルIPアドレスが割り当てられる	2017/05/04
HX008ZT(Willcom)	Softbank 004Zとほぼ同じ？	検証予定	-
Doccica BM-DC1-500M(b-mobile)	ZTE MF636として認識 Doccica（ドッチーカ）詳細仕様 | b-mobile Doccica ※標準SIMじゃないと挿しにくい	○ Docomo SIMで3G接続確認。moperaであればppp-outにグローバルIPアドレスが割り当てられる	2017/05/04

ドングルでなくてもいいのでは?
左：W04　右：W03

hAP acにUSB接続できる技適のあるLTEデバイスを見つけた

Speed Wi-Fi NEXT W03 HWD34 / W04 HWD35
(UQ mobile版もあり)

→　AUのWiMAX 2+対応モバイルルーター
製造はHuawei（HiLinkルーター）

→　AUに中古端末を持ち込んで契約することができない（ので、中古端末が非常に安い)

→　SIMロックがかかっていない

※W05はSIMの種類が少し変更になっているのであまりおすすめしません

可搬型Hotspot 2.0/Passpoint基地局
MikroTik hAP acバージョン

要件：　ブランチ拠点の通信は全てVPN経由でセンター拠点に流したい

環境：　センター拠点側はグローバルIPアドレス（固定）ブランチ拠点側はLTE接続でISPシェアードアドレス（100.64.0.0/10）が割り当てられている

※回線はIIJmio タイプA

hAP acに接続したW04のLTE回線経由で、センター拠点のhEXにOpenVPNで接続してみよう

■事前準備

センター拠点側（hEx）

- ether1で光ネクスト回線にPPPoE接続(pppoe-out1)
- ether2に172.16.2.1を設定
- ether2-ether5までブリッジ設定
- ファイアウォール設定
- sntp-clientの設定

ブランチ拠点側（hAP ac）

- USBポートにW03接続済（W03/W04ではポートは開けない）→　lte1となる
- sntp-clientの設定
- ファイアウォール設定

[admin@MikroTik] > /system resource usb print detail
 0 device=“1-0” vendor=“Linux 3.3.5 ehci_hcd” name=“RB400 EHCI” serial-number=“rb400_usb”
    vendor-id=“0x1d6b” device-id=“0x0002”speed="480" ports=1 usb-version=" 2.00"

 1 device="1-1" vendor="HUAWEI_MOBILE" name="HUAWEI_MOBILE"
   vendor-id="0x12d1" device-id="0x14db" speed="480" usb-version=" 2.00"

[admin@MikroTik] > /port print detail
Flags: I - inactive

センター拠点側 OpenVPN設定

センター拠点側でCA作成
CA証明書をエクスポート
センター拠点（VPNサーバ）用とブランチ拠点（VPNクライアント）用の公開鍵と秘密鍵のペアを作成
公開鍵を作成したCA証明書で署
ブランチ拠点用の公開鍵と秘密鍵、証明書をエクスポート
winboxのFiles、またはsftp接続などでブランチ拠点用のファイルをダウンロード
pppプロファイルとipアドレスプールを作る
（センター拠点側を=172.16.2.3とし、ブランチ拠点側を172.16.2.4から払い出す。）

ブランチ拠点用のpppユーザを作成

センター拠点にOpenVpn Serverのインターフェース作成
L2VPNにしたいのでmodeはethernetにする
AU網ではTCP1194が通信遮断されるため、標準のTCP:1194は利用しない

ovpn-centerをブリッジに追加
センター拠点へのOpenVPNポートの通信を許可
（現状、RouterOSではOpenVPNで使用できるのはTCPのみ、UDPではVPNを張れない）

ブランチ拠点側 OpenVPN設定

winboxのFilesから、センター拠点で作成してダウンロードした
ブランチ拠点用のファイルをアップロード

証明書をインポート
OpenVPN Clientインターフェースを作成
ovpn-out1をブリッジに追加

DHCPサーバは止める（VPNクライアント側の端末は、センター拠点の
DHCPからIPアドレスを払い出す）

LTEでau網を使う場合は、MTUに注意（W03/04側でも調整してくれる）
網のMTUは1420byte、MSSは1380

接続確認

センター拠点側

[admin@MikroTik] > /log print
22:41:11 ovpn,info TCP connection established from x.x.x.x
←ここはLTE接続のプロバイダのグローバルIPアドレスになっている
22:41:15 ovpn,info : using encoding - AES-256-CBC/SHA1
22:41:15 ovpn,info,account branch logged in, 172.16.2.4
22:41:16 ovpn,info <ovpn-branch>: connected

ブランチ拠点側

22:41:11 ovpn,info ovpn-out1: initializing...
22:41:11 ovpn,info ovpn-out1: connecting...
22:41:16 ovpn,info ovpn-out1: using encoding - AES-256-CBC/SHA1
22:41:16 ovpn,info ovpn-out1: connected

可搬型Hotspot 2.0/Passpoint基地局
MikroTik hAP acバージョン

完成

バッテリー駆動でAC電源不要
OpenVPNでRADIUS認証情報と
ユーザートラフィックは全て
センター拠点に

バックボーンはUSB接続のW04
(技適アリ 有線LAN部分がないのでより安心

可搬型Hotspot 2.0/Passpoint基地局
MikroTik hAP acバージョン

City Wi-Fi Roaming 2018

Coming soon

http://worldwifiday.com/city-wi-fi-roaming/

OPERATORS AROUND THE WORLD INCLUDE:

2 Degrees New Zealand • AT&T • Airtel • AIS Thailand • Bell Mobility • BT • Celcom Axiata Berhad • China Mobile • csl Hong Kong

NGH Special Interest Group (NGHSIG)
http://nghsig.jp