The Co-located Hotspot in the Residential Gateway

Jan Önnegren
Ericsson
Sweden

Anna Olszewska-Olbryś
Telecom Poland Research and Development Center
Poland

Alex De Smedt
Thomson Telecom
Belgium

Jan Önnegren

BroadBand Europe
3-6 December '07
Antwerp, BELGIUM

Multi Service Access Everywhere
Contents

> Introduction to Co-located hotspot
> The business model
> How Users connects to a Co-located Hotspot (example)
> Co-located Hotspot Architectures
> Authentication solutions
> Access restrictions in RGW for hotspot users
> Functions needed in RGW
> Conclusions
Introduction to Co-located hotspot

Add Hotspot functionality in the RGW so that it directs flows to a hotspot NSP (fixed or mobile) offering IP-based services.
The business model

Virtual-Hotspot gateway provider

Hotspot provider

NSP

Regulator

Internet/Applications

Advantage

k uses

m agreement/contract for Hotspot usage

n allows 1 contract for Hotspot function

card

1 licenses
How Users connects to a Co-located Hotspot (example)

Beacons (WiFi-Telop)
How Users connects to a Co-located Hotspot (example)
How Users connects to a Co-located Hotspot (example)

User may need to enter billing information

Authentication ex. EAP-AKA

Hotspot-VLAN
How Users connects to a Co-located Hotspot (example)

User can access Internet
AAA architecture consists of:

- Supplicant able to communicate using authentication protocol
- Authenticator able to contact AAA server in the network
- access policy Enforcement Point (EP) in initial state blocks all traffic with exception of authentication related traffic

- Authentication traffic goes through EP
- EP enables Internet traffic after successful authentication
Co-Located Hotspot Architecture 2(4): EAP framework

- **EAP framework consists of:**
  - Peer (supplicant) implementing an EAP peer
  - Pass-through authenticator implementing EAP authenticator
  - Authentication server (AAA server) also implementing EAP authenticator

---

<table>
<thead>
<tr>
<th>EAP method</th>
<th>Authentication protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP</td>
<td>802.1X, PANA, IKEv2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EAP method</th>
<th>AAA protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP</td>
<td>RADIUS, Diameter</td>
</tr>
</tbody>
</table>

**AAA server**

**Pass-through authenticator**

**Supplicant**
> Mapping to Hotspot Architecture:

- Supplicant is the UE containing Wi-Fi (802.11)
- Pass-through authenticator is placed in the Access Controller (AC) for the hotspot
- Enforcement Point (EP) can be located in the Access Controller (AC) or it can be separated from the AC (Option in PANA)
- AAA-Server in Hotspot NSP network
Co-Located Hotspot Architecture 4(4): Solutions

Case | Wi-Fi UE | RGW
--- | --- | ---
A | 1 | AP
2 | Example: i-WLAN
3 | Example: PANA
B | 4 | Web-based Example
- PANA
C | 5 | Web-based Example
- CAPWAP

- Broadband Access Network
- Regional/ Core IP network
- NSP1-Hotspot

Example:
- WPA2 Enterprise, I-WLAN

4 Dec 2007

Co-located hotspot in RGW
Page 12
Authentication solutions 1(3): Case A

Case A: AP in RGW ➔ encryption on L3, secure

PANA - RADIUS

I-WLAN - Diameter

Data tunneling!
To fixed network

Data tunneling!
To mobile network

End session for IKEv2 and PANA

End session for IKEv2
Authentication solutions 2(3): Case B

Case B: WTP in RGW ➔ encryption on L2, tunneling on L3, secure

CAPWAP (Split MAC)

CAPWAP= Control and Provisioning of Wireless Access Points (IETF)
Two versions exists:
- Split MAC
- Local MAC

Dedicated for Public Hotspots
Authentication solutions 3(3): Case C

Case C:
- AP/EP/AC in RGW
- Trusted RGW needed

Wi-Fi Encryption!
Access restrictions in RGW for hotspot users 1(2)

> Basic Principle:
Hotspot traffic fills up the UNUSED Bandwidth on the access line

The RGW needs to assure:
> Limitation of number of hotspot users
  E.g. 2-3 maximum
> Limitation of the maximum bandwidth
  E.g. H% of total BW
> QoS settings for hotspot users (possible to have “Tuned solutions”)
Access restrictions in RGW for hotspot users 2(2)

Limitation of bandwidth for Hotspot traffic

\[ H\% = \text{max % that can be used by hotspot} \]

Hotspot traffic

\[ 100\% \]

Hotspot traffic is limited due to that maximum (H\%) is reached

Hotspot traffic is limited due to high Home user traffic

\[ (100-H)\% \]

\[ 100\% \]

Case-1: Hotspot users have no guaranteed minimum bandwidth
> RGW with Co-located hotspot functionallity must support:
  
  - **Separation of CPN and Hotspot traffic** (Multiple SSID support)
  - **Hotspot control**: Monitor hotspot traffic (logging of activities) and apply access restrictions (no of users, QoS settings and bandwith limitations)
  - **Aggregate all hotspot traffic** to the Fixed/Mobile Hotspot NSP
  - **Remote management**: Control and Management

> RGW may need to support (depending on selected "solution")
  
  - EAP pass-through authenticator, WTP functionallity, Support for different tunnel (IPSec), provide local (unauthorised) IP address…
A deeper look into the RGW….for Case C

- Functions needed in RGW 2(2)
  
  **Functions needed in RGW 2(2)**

  - A deeper look into the RGW….for Case C

  - **PHY**
    - Ethernet
    - Configuration and management
    - Session/accounting communication
    - Upload log files
  - **802.1x**
    - IP: Wi-Fi ass to SSID
    - IP: 802.1x
    - IP: DHCP
    - IP: EAP pass-through
    - IP: NAPT + IP forwarding
    - VLAN
    - Ethernet
    - Auth
    - IP config
    - Data transfer
  - CAC, IP-QoS, Firewall and Filtering
  - Blocking traffic to home network
  - Session monitoring/ Logging NAPT
  - Upload log files

**Co-located hotspot in RGW**

**Page 19**
Conclusions

> The co-located hotspot offers a win-win situation for hotspot provider, home user and travellers

> Filling up the otherwise unused bandwidth is the main issue

> Advised:
  - Authenticator is not in RGW
  - Data transfer is secured (encrypted/tunnelled)
  - Logging of sessions for legal reasons

> Preferred solutions:
  - WPA2 (+CAPWAP) as a short solution
  - PANA or I-WLAN + tunnelling as a long term solution
Thank you!

Questions?