| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>** |
| Title | **Network Entry Through an RS with Distributed Security** |
| Date Submitted | **2007-09-09** |
| Source(s) | Hang Zhang, Peiying Zhu, Mo-Han Fong, Wen Tong, David Steer, Gamini Senarath, G.Q. Wang, Derek Yu, Israfil Bahceci, Robert Sun and Mark Naden<br>Nortel<br>3500 Carling Avenue<br>Ottawa, Ontario K2H 8E9<br>Voice: +613-763-1315<br>E-mail: wentong@nortel.com<br>Voice: +613-765-8983<br>E-mail: pyzhu@nortel.com |
| Re: | IEEE P802.16j/D1: IEEE 802.16j working group letter ballot #28 |
| Abstract | For the distributed security case, the security materials of a MS attached to an access with distributed security are accessible and kept by the access RS. Such an RS can locally process MS's messages. This contribution clarifies the description about the MS initial network entry via an access RS with distributed security |
| Purpose | To incorporate the proposed text into the P802.16j/D1 Baseline Document |
| Notice | *This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<br><http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<br><http://standards.ieee.org/guides/opman/sect6.html#6.3>.<br>Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>. |

# Network Entry through an RS with Distributed Security

*Hang Zhang, Peiying Zhu, Mo-Han Fong, Wen Tong, David Steer, Gamini Senarath, G.Q. Wang, Derek Yu, Israfil Bahceci, Robert Sun and Mark Naden*

*Nortel*

## 1. Introduction

In current baseline document, both centralized security and distributed security scenarios are described. In distributed security case, the security materials of a MS attached to an access with distributed security are accessible and kept by the access RS. Such an RS can locally process MS's messages. Thus the MS initial network entry process is different from the process in centralized security case. Currently, the description about the MS initial network entry via an access RS with distributed security is missing. This contribution provides this process.

## 2. Proposal

For MS initial network entry, some messages such as RNG-REQ/RSP and SBC-REQ/RSP can be locally processed first then the attachment of a MS is informed to the MR-BS. The information carried in messages such as PKM-REQ/RSP and REG-REQ/RSP need to be forwarded to MR-BS and the corresponding response of MR-BS needs to be forwarded to MS. The MS initial network entry through an RS with distributed security is illustrated in Figure 1.

The procedures are described as followings:

- DL/UL synchronization
  - For DL synchronization, no any additional requirement for an access RS
  - During MS UL synchronization, the RS shall locally assign a basic CID and a primary CID to the MS
  - After the MS DL/UL synchronization, the RS may send RS_MSG_Relay-REQ message to MR-BS which include the TLVs of RNG-REQ/RSP (those TLVs may be transmitted to MR-BS after SBC-REQ/RSP exchange)
    - SS MAC Address
    - Basic CID and primary CID (locally assigned to the MS)
  - The MR-BS shall response with RS_MSG_Relay-RSP message
    - No TLV of RNG-RSP TLV is included
  - After the MS DL/UL synchronization, the MR-BS establishes a binding between the MS ID and the basic CID and primary CID locally assigned by the RS
- Basic capability negotiation
  - A MS and an access RS negotiate the basic capability locally through SCB-REQ/RSP messages without involvement of MR-BS
  - After the negotiation between the MS and the RS, the RS shall send RS_MSG_Relay-REQ message to MR-BS. The following TLVs of SBC-REQ message may be included
    - Security Negotiation Parameters
  - MR-BS shall send RS_MSG_Relay response message to the access RS as a response to RS_MSG_Relay-REQ sent from the access RS
    - No TLV of SBC-REQ/RSP TLV is included
  - The RS_MSG_Relay-RSP message may includes the TLVs of RNG-REQ/RSP messages if the access RS decides to combine those information together

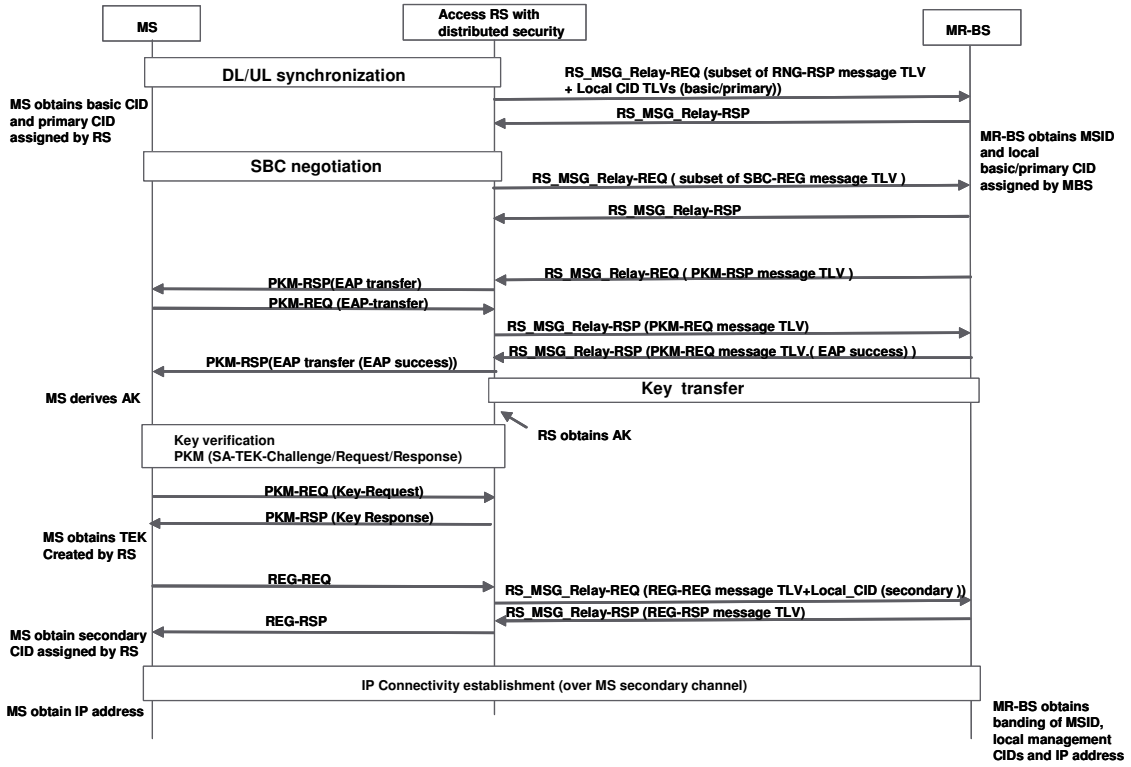


Figure 1. An example of MS initial network entry through an RS in moving BS mode.

- MS authorization/authentication (EAP case) and key establishment
  - The MR-BS may trigger the MS authorization/authentication by sending RS_MSG_Relay-REQ message to an access RS including the fields of PKM-RSP and
    - EAP transfer attributes of PKMv2 EAP Transfer message
  - The access RS creates PKM-RSP message by including the above contents and sends to the MS
  - The MS sends the PKM-REQ (PKMv2 EAP Transfer) message to the access RS
  - The access RS then creates RS_MSG_Relay message by including following
    - fields of PKM-REQ (PKMv2 EAP Transfer) received from the MS
    - EAP transfer attributes of PKMv2 EAP Transfer message received from the MS
  - After the AK of the MS is available by MR-BS, the MR-BS shall deliver the AK through AK transfer
  - The access RS and the MS then shall use PKMv2 3-way handshake to verify the AK and use PKMv2 Key-request/Reply exchange to make the MS obtain valid TEK keys. These message exchanges happen between the access RS and MS only without MR-BS involvement
- MS registration to the network
  - MS sends the REG-REQ message to the access RS. The RS shall include the following TLVs from the received REG-REQ message in RS-MSG_Relay-REQ and send this RS_MSG_Relay-REQ to MR-BS:
    - IP version
    - Vendor ID encodings
    - Vendor-specific information
    - Secondary CID locally assigned by the access RS

- MR-BS creates RS_MSG_Relay-RSP message by including the following TLVs of REG-RSP message:
  - IP version
  - Vendor ID encodings
  - Vendor-specific information
- Access RS creates the REG-RSP message to the MS

- MS IP connection establishment
  - All MS IP connection related protocol messages are viewed as a type of service flow with an assigned QoS class. Those messages are exchanged between the MR-BS and the MS though the MS's local secondary connection over the forwarding transport connection (F-CID) between the access RS and the MR-BS

## 3. Proposed text change

3.1 Description of MS initial network entry

*[Add the section 6.3.9.16.5 as followings]*
++++++++++++++ Start text ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

6.3.9.16.5 Network entry of MS through an access RS in moving BS mode (MBS)

For MS initial network entry though an access RS with distributed security, some messages such as RNG-REQ/RSP and SBC-REQ/RSP can be locally processed first then the attachment of a MS is informed to the MR-BS. The information carried in messages such as PKM-REQ/RSP and REG-REQ/RSP need to be forwarded to MR-BS and the corresponding response of MR-BS needs to be forwarded to MS. The MS initial network entry through an RS with distributed security is illustrated in Figure XXX.

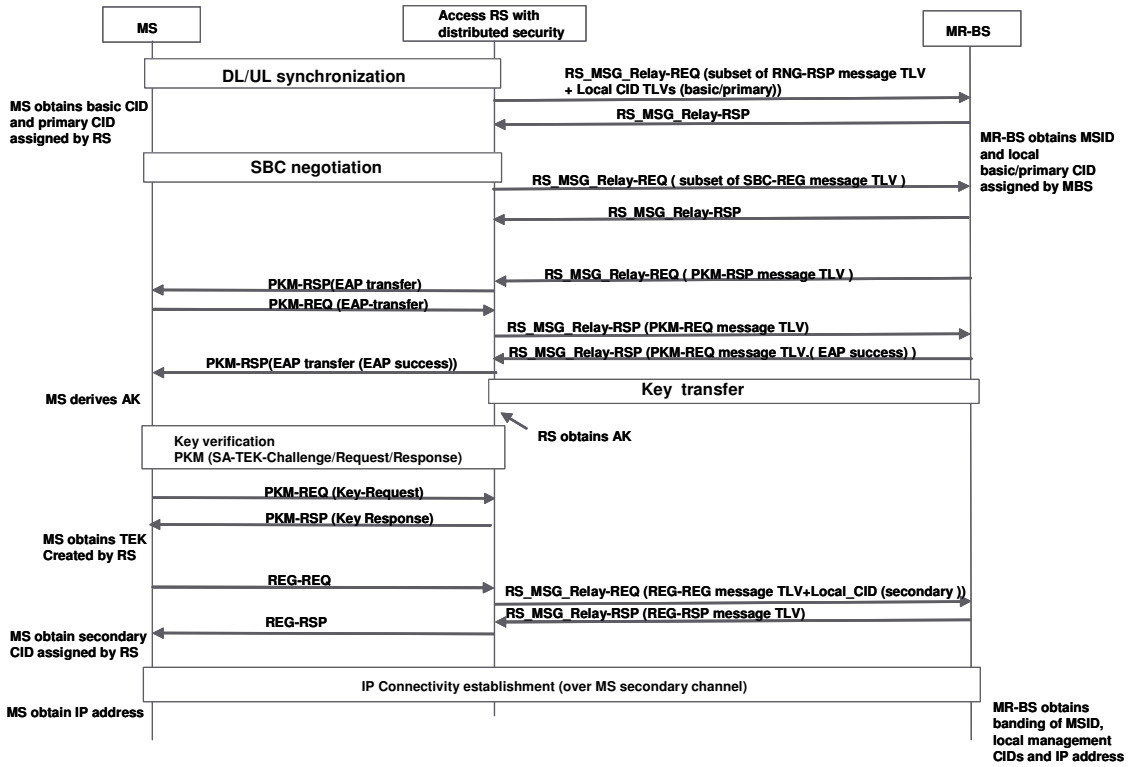

Figure xxx. An example of MS initial network entry through an RS in moving BS mode.

The procedures are described as followings:

- DL/UL synchronization
  - For DL synchronization, no any additional requirement for an access RS in moving BS mode
  - During MS UL synchronization, the RS shall locally assign a basic CID and a primary CID to the MS
  - After the MS DL/UL synchronization, the RS may send RS_MSG_Relay-REQ message to MR-BS which include the following TLVs of RNG-REQ/RSP (those TLVs may be transmitted to MR-BS after SBC-REQ/RSP exchange)
    - SS MAC Address
    - Basic CID and primary CID (locally assigned to the MS)
  - The MR-BS shall response with RS_MSG_Relay-RSP message
    - No TLV of RNG-RSP TLV is included
  - After the MS DL/UL synchronization, the MR-BS establishes a binding between the MS ID and the basic CID and primary CID locally assigned by the RS
- Basic capability negotiation
  - A MS and an access RS negotiate the basic capability locally through SCB-REQ/RSP messages without involvement of MR-BS
  - After the negotiation between the MS and the RS, the RS shall send RS_MSG_Relay-REQ message to MR-BS. The following TLVs of SBC-REQ message may be included
    - Security Negotiation Parameters
  - MR-BS shall send RS_MSG_Relay response message to the access RS as a response to RS_MSG_Relay-REQ sent from the access RS
    - No TLV of SBC-REQ/RSP TLV is included
  - RS_MSG_Relay-RSP message may includes the TLVs of RNG-REQ/RSP messages if the access RS decides to combine those information together with those of SBC-REQ/RSP
- MS authorization/authentication (EAP case) and MS key establishment
  - The MR-BS may trigger the MS authorization/authentication by sending RS_MSG_Relay-REQ message to an access RS including the fields of PKM-RSP and
    - EAP transfer attributes of PKMv2 EAP Transfer message
  - The access RS creates PKM-RSP message by including the above contents and sends to the MS
  - The MS sends the PKM-REQ (PKMv2 EAP Transfer) message to the access RS
  - The access RS then creates RS_MSG_Relay message by including following
    - fields of PKM-REQ (PKMv2 EAP Transfer) received from the MS
    - EAP transfer attributes of PKMv2 EAP Transfer message received from the MS
  - After the AK of the MS is available by MR-BS, the MR-BS shall deliver the AK through AK transfer to the access RS
  - The access RS and the MS then shall use PKMv2 3-way handshake to verify the AK and use PKMv2 Key-request/Reply exchange to make the MS obtain valid TEK keys. These message exchanges only happen between the access RS and MS without the involvement of MR-BS
- MS registration to the network
  - MS sends the REG-REQ message to the access RS. The RS shall include the following TLVs from the received REG-REQ message in RS-MSG_Relay-REQ and send this RS_MSG_Relay-REQ to MR-BS:

        - IP version
        - Vendor ID encodings
        - Vendor-specific information
        - Secondary CID locally assigned by the access RS
    - MR-BS creates RS_MSG_Relay-RSP message by including the following TLVs of REG-RSP message:
        - IP version
        - Vendor ID encodings
        - Vendor-specific information
    - Access RS creates the REG-RSP message and sends the message to the MS
- MS IP connection establishment
    - All MS IP connection related protocol messages are viewed as a type of service flow with an assigned QoS class. Those messages are exchanged between the MR-BS and the MS though the MS's local secondary connection over the forwarding transport connection (F-CID) between the access RS and the MR-BS

++++++++++++++ End text ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

3.2 RS_MSG_Relay-REQ message encodings

*[Please insert the following to the end of 11.27 RS_MSG_Relay-REQ/RSP message encodings]*

++++++++++++++ Start text ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

11.27 RS_MSG_Relay-REQ/RSP message encodings

The RS-MSG_Relay-REQ/RSP message encodings are shown in Table XXX.

Table XXX. RS-MSG_Relay-REQ/RSP message encodings

| Name | Type | Length | Value | Scope |
|---|---|---|---|---|
| Locally assigned basic/primary connection CIDs | 1 | 4 | Bytes 0-1: basic connection CID locally assigned by an access RS<br>Bytes 2-3: Primary connection CID locally assigned by an access RS | RS_MSG_Relay-REQ/RSP |
| Locally assigned secondary connection CID | 2 | 2 | Secondary connection CID locally assigned by an access RS | RS_MSG_Relay-REQ/RSP |

11.27.1 Locally assigned basic/primary connection CIDs

This TLV is used for an access RS in moving BS mode to inform MR-BS its locally assigned basic connection CID and primary connection CID to a MS.

11.27.2 Locally assigned secondary connection CID

This TLV is used for an access RS in moving BS mode to inform MR-BS its locally assigned secondary connection CID to a MS.

++++++++++++++ End text ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++