Authentication Letter Ballot comments

Wim Diepstraten
AT&T WCND
Nieuwegein
The Netherlands
Authentication discussion

- This document intends to analyse the functionality of the different authentication schemes that are currently defined in D2 draft, and tries to identify the differences in their characteristics

- There are 3 authentication mechanisms defined:
  - Open Authentication
  - Shared Key authentication
  - Proprietary authentication

- Basic assumptions.
  - The objective for the 802.11 authentication is simply used to bring the wireless link up to the assumed physical standard of a wired link (section 2.4.3.1 par 5)
    » So "Open Authentication" that compares the STA address against a "Allowed List" does achieve this basic function.
    » But a station could fraud to be another station by using its SA address.
  - More sophisticated Authentication does only make sense when Privacy is used on all data traffic, so when WEP is on.
    » otherwise stations can always fake to be an other station to send its information anyway.
  - If WEP is not used, then a more sophisticated Authentication scheme does not prevent stations to fake identity.
  - If a station does know the WEP key, then that is equivalent to a station being physically connected to the wired medium.
    » So then we have achieved the spirit of the "Wired Equivelancy".

- So when WEP=on then knowledge of the WEP key does accomplish the "Wired Equivelancy", and provide a level of implicit authentication.
Authentication examples:

```
<table>
<thead>
<tr>
<th>STA1</th>
<th>STA2 = AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: I am SA, open Auth</td>
<td>Auth via AP-SA List</td>
</tr>
<tr>
<td></td>
<td>No Auth.</td>
</tr>
<tr>
<td>A2: OK Auth accepted-&gt;S2</td>
<td>SA List in AP</td>
</tr>
<tr>
<td>Associate Req</td>
<td></td>
</tr>
<tr>
<td>Associate Response --&gt;S3</td>
<td></td>
</tr>
<tr>
<td>Data or Data(WEP)</td>
<td></td>
</tr>
</tbody>
</table>
```

If WEP on, then correct Key ownership is implicit Authentication.

**Open System Authentication**

- **Open System Authentication:**
  - Either no Authentication or
  - AP can verify allowed membership against SA list.
  - This makes sense with WEP = off.
  - but does not protect against fake identity.

- **When WEP=on then** knowledge of same key on both end is required to allow communication.
  - So this is implicit authentication.
  - If Station is not who he claims to be does not make any difference for privacy, because it has the key, so it can see all traffic.

- **So Implicit authentication makes a lot of sense from a privacy point of view.**
  - It does accomplish the "Wired Equivelancy" goal.
Shared Key Authentication:

- **Shared Key Authentication:**
  - Needs WEP algorithm + Shared Key in Authentication phase.
  - The same key is used for Privacy and Authentication (no separate key provisions in MIB).
  - AP can do an additional membership check against SA list.
  - Using Shared Key Authentication, without using WEP for data privacy does not make sense from privacy point of view. (We are not doing security but privacy).
- So Shared Key Authentication does also rely on knowledge of the same key on both ends.
- What is the value of Shared Key versus Open System Authentication when WEP is on????????
  - So why bother?

Conclusion: Shared Key authentication is equivalent to Open System authentication, because they both depend on the knowledge of the same key on both ends.

Recommendation: Delete Shared Key Authentication method.
Proprietary Authentication:

Proprietary Authentication algorithm

- Proprietary algorithm possible.
  - Can take relative long time depending on algorithm.
  - Therefore desire for pre-authentication possibility.
  - Station can be authenticated with multiple APs and Stations at the same time according to current scheme.
    » This is basic requirement to allow pre-authentication.

- There is a desire for support of other authentication methods.
  - This is provided by the mechanism as currently defined.
  - Although from a privacy point of view it does not provide additional protection when the WEP key is known.
Maintaining Authentication State:

- Stations need to be able to be authenticated with multiple stations at the same time.
  - Basically to allow pre-authentication to prevent long proprietary authentication delays.
- Currently each TA/RA pair must maintain a authentication state variable.
  - Authentication is needed before any traffic can occur between a given station (TA/RA) pair.
  - For an AP this is no problem, because it needs to maintain per station knowledge for all kind of purposes.
  - For a Station in an IS this is default no problem, as long as all traffic is going via the AP (DS).
  - In Ad-Hoc a Station does need to maintain State information for all stations it wants to communicate with.
  - The same is true for a Station in an IS that wants to do direct S-to-S traffic, then it needs to maintain extra Authentication State information for each station that wants to communicate directly, in addition to the AP.
- Effect of Authentication requirement for S-to-S.
  - First transmission to a given station should be a Authentication handshake.
  - If there is a mismatch between state information on both ends then traffic is dropped (although Acked), and there is no feedback about this occurring.
  - Similar to suggested changes in AP, rules could be changed such that if such is detected, then a station has to do a deAuthenticate, to get state information on both ends in line.
  - However do we need/want this complexity??
- Authentication and WEP was there primarily to protect the DS, and to prevent to compromise the privacy of the existing wired network.
  - For Ad-Hoc implicit authentication is achieved when WEP is used.
  - This is more then sufficient for Ad-Hoc.
Implicit Authentication in Ad-Hoc

- Conclusion:
  - Implicit Authentication is enough for Ad-Hoc.
  - So no explicit authentication is needed.
  - So no S-to-S state information needs to be maintained.
    - which is an N to N problem.
  - Complexity reduction for Stations.
  - This is accomplished by allowing S-to-S traffic in State 1 of Figure 2-8. (To_DS = off).

- This can also simplify the Association:
  - Define an Authentication field in the (Re)Association frames.
    - This can have the value:
      - Pre-authenticate
      - Open System
      - Or "Shared Key" if not deleted.
    - If value is Pre-Authenticate, then an explicit Authentication cycle is needed.
    - If value is open System, then Association can proceed as normal.
      - Only returning status should show separate authentication failure code.
  - Association is reduced to two frames.
  - pre-authentication is still possible.

Conclusion:

- Using implicit "authentication only" for Ad-Hoc allows combined Association/Authentification frames without any loss of capability / flexibility.
- Also applies to any traffic with To_DS and From_DS both false

Recommendation: Authentication is not needed for Ad-Hoc. So allow direct data frames (To_DS and From_DS both false) also as Class-1 frame.