|  |  |  |  |
| --- | --- | --- | --- |
| Network Detection and Selection Text Example | | | |
| Date: 2014-01-23 | | | |
| **Authors:** | | | |
| Name | Affiliation | Phone | Email |
| Maximilian Riegel | NSN | +49 173 293 8240 | maximilian.riegel@nsn.com |
|  |  |  |  |
|  |  |  |  |
| **Notice:**  This document does not represent the agreed view of the OmniRAN EC SG. It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein. | | | |
| **Copyright policy:**  The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>. | | | |
| **Patent policy:**  The contributor is familiar with the IEEE-SA Patent Policy and Procedures:  <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. | | | |

# Abstract

The contribution presents initial text proposal for the Network Detection and Selection section of the recommended practice. The proposals inherit thoughts and structure from the WiMAX Forum NWG Stage 2 specification.

# Network Discovery and Selection

# AN, control entity Domains

The adopted network reference model enables deployments wherein an STA may encounter one or more of the following situations:

1. An Access Network (AN) owned by a single control entity (also referred to as ‘integrated AN’ deployment case).
2. An AN owned by a single entity but collectively deployed by two or more control entities (also referred to as “AN sharing” deployment case).
3. A region covered by two or more ANs, representing either the “integrated AN” or the “AN sharing” scenario.

The STA SHOULD be enabled to discover all accessible control entities, and SHOULD be able to indicate the selection of the preferred control entity during the establishment of connectivity to the AN. The actual selection mechanism of the control entity employed by the STA MAY be based on various preference criteria, possibly depending on the presence of preconfigured configuration information in the STA.

Preconfigured configuration information in the STA SHOULD include:

1. Information useful for discovery of ANs including channel, center frequency, and PHY profile,
2. information useful for discrimination and prioritization of control entities for service selection including a list of authorized ANs and a list of authorized control entities with a method of prioritization for the purpose of automatic selection,
3. a list of authorized ‘share’ or ‘roaming’ affiliation relationships between authorized ANs and control entities and partner ANs and control entities, with a method of prioritization for the purpose of automatic selection, and
4. identity/credentials provided by control entity to which the STA has a trust relationship.

The details of provisioning of configuration information is out of scope of this specification. It may be provided on a pre-provisioned basis or at time of dynamic service subscription of a STA and may be subject to periodic update in a method outside the scope of this standard.

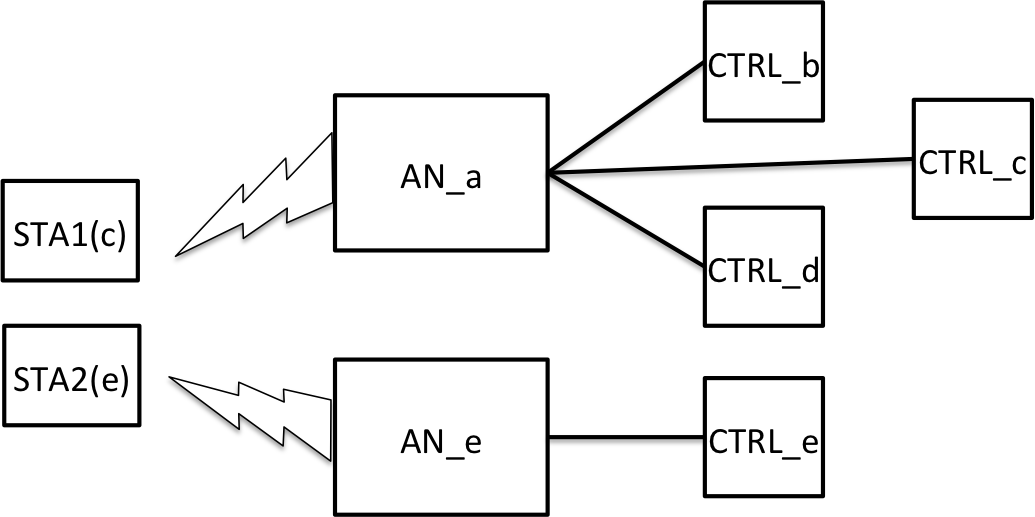


Figure 1 - Coverage Area with Overlapping ANs

For example, as shown in Figure 1, STA1 and STA2 discover available control entities and select one based on its configuration information. More specifically, STA1 prefers to connect to AN\_a of because it is directly affiliated with STA1’s home control entity CTRL\_c through AN sharing. And, STA2 prefers to connect to AN\_e because it is owned by STA2’s home control entity CTRL\_e.

A solution framework SHOULD enable STAs to discover the identities of available control entities accessible in a particular IEEE 802 access network coverage area, and indicate their selected control entities to the AN, to which they connect to.

# Use Case Scenarios

Access network discovery and selection procedures are usually executed when a STA is used for the first time, for initial network entry after powering on, for network re-entry, when the STA lost connectivity to the previous AN, or when an STA transitions across AN coverage areas. This subsection describes all four use case scenarios.

## 1. First-time use of STA without control entity identity information available

1. STA detects one or more available ANs.
2. STA discovers available control entities associated with one or more ANs.
3. STA identifies all accessible control entities and selects an AN and an control entity based on some preference criteria.
4. STA performs a special connection procedure with the selected AN for initialization of a subscription.
5. STA becomes authorized on the selected control entity for service subscription only for the purpose to create a trust relationship with the selected control entity.
6. STA creates a trust relationship enabling network access authentication and authorization by the selected control entity.
7. STA acquires and stores the configuration information of the selected control entity.

## 2. Initial network entry after power-on or first-time use of new configuration information

1. STA detects, using the stored configuration information, one or more available ANs.
2. STA discovers available control entities associated with one or more ANs.
3. STA identifies all accessible control entities and, using the stored configuration information, selects or allows a subscriber to select an control entity based on some preference criteria.
4. STA performs an initial network entry procedure with a AN that is supported by selected control entity.

In case of failure, STA reverts to Use Case scenario 1.

## 3. Network re-entry

Network re-entry is equivalent to establishing connection with the same or another access point of the previously connected AN. Scenario 3 procedures assume that AN and control entity maintain their relationship.

In case of failure, STA reverts to scenario 2.

## 4. STA transitions across multiple AN coverage area

1. STA has previously completed network entry and is in normal operation with its control entity on an AN.
2. STA discovers, using the stored configuration information, one or more available neighboring ANs.
3. STA discovers that the neighboring ANs have direct or indirect relationships with the same control entity, by which it is currently authenticated and authorized.
4. Due to user movement or other reason, the STA decides to transition to another AN.
5. STA performs an network re-entry procedure with an neighbor AN that has a relationship to the currently used control entity enabling access by the same control entity. This network re-entry will involve a full authentication cycle to re-establish a complete session context with the new AN.

In case of failure, STA reverts to scenario 2.

# Discovery and Selection of AN and Control Entity

This subsection presents the procedures for discovery and selection of AN and control entity.

The solution consists of four procedures:

1. AN Discovery
2. Control Entity Discovery
3. Control Entity Enumeration and Selection
4. AN Attachment

*AN Discovery* refers to a process wherein a STA discovers available AN(s) in its surrounding. *Control Entity* Access *Discovery* refers to the process wherein a STA discovers available control entity(s) deploying the ANs in its surrounding. *Control Entity Enumeration and Selection* refers to a process of choosing the most preferred control entity and a candidate set of ANs to attach to, based on the dynamic information obtained during the discovery phase and information stored in the STA. *AN Attachment* based on *Control Entity* *Enumeration and Selection* refers to the process wherein the STA indicates its selection decision during connection establishment with an AN deployed by its control entity by providing its identity (potentially in the form of NAI). The enumerated steps are not sequential and need not be completed in their entirety. That is, *Control Entity Access Discovery* and *Control Entity Enumeration and Selection MAY* well be performed by the STA concurrent torunning *AN Discovery* procedures. Also, there is no requirement that an STA SHOULD discover ***all*** ANs and control entities in the accessible environment. An STA MAY terminate the discovery process once an AN and a control entity is discovered, which meet the *Control Entity Enumeration and Selection* criteria of the STA. After preempting the discovery process the STA SHOULD proceed with the *AN Attachment* procedure.

# Access Technology specific Procedures

## IEEE 802.3

For further study.

## IEEE 802.11

For further investigation.

## IEEE 802.15

For further study.

## IEEE 802.16

### AN Discovery

An STA detects available AN(s) by scanning and decoding DL-MAP of AN(s) on detected channel(s). The 24-bit value of the “operator ID” (see 6.3.2.3.2 of IEEE Std 802.16) within the “Base Station ID” parameter in the DL-MAP message is the AN Identifier and is used to indicate the ownership of the AN. The value of the 24-bit “operator ID” SHOULD be assigned as an IEEE Std 802.16 Operator ID by the IEEE Registration Authority. Operator ID/AN ID allocation and administration method, and field formatting are defined in IEEE Std 802.16. If information useful in STA discovery of AN is available in configuration information, it MAY be used to improve efficiency of AN discovery.

### Control Entity Access Discovery

The AN SHOULD be served by one or more control entities. In control entity discovery, a control entity identifier can be presented to the STA as a unique 24 -bit control entity identifier. The value of the 24 -bit control entity ID (i.e., control entity Identifier) SHOULD be issued as an IEEE Std 802.16 Operator ID by the IEEE Registration Authority4. As both AN ID and control entity ID are allocated from the same number space, the numbers are guaranteed to be unique in both domains. Control entity ID is either a 22-bit globally-assigned ID or a combined MCC+MNC as described in ITU-T Recommendation E.212. Selection of the method used for control entity ID format is implementation specific.

If the STA cannot derive available control entities during scanning from the AN identifier out of the control entity Identifier Flag, detected AN IDs, and the configuration information, then it SHOULD try to dynamically discover a list of control entities supported by the AN.

If the AN and control entity are the same (i.e., there is a one-to-one relationship between these IDs), the AN SHOULD identify this case by setting the least significant 1st bit (1st LSB; the 25th bit of Base Station ID; the control entity Identifier Flag) of the Base Station ID to a value of ‘0’. For this case, the STA SHOULD assume that the control entity ID is the same ID presented as AN ID.

In the event that more than one control entities are served by a detected AN, or that some regulatory or deployment requirement compels separate presentation of one or more control entity IDs, the AN SHOULD identify this case by setting the control entity Identifier Flag to a value of ‘1’.

Independently of control entity Identifier Flag value, the AN MAY transmit the control entity ID list and verbose control entity Name List as part of the Service Information Identity (SII-ADV) broadcast MAC management message. Also, the BS SHOULD transmit the list of control entity IDs and Verbose control entity Names as part of SBC-RSP in response to an STA request through SBC-REQ.

If the list of control entity identifiers supported by a AN does not exist in the configuration information of the STA in this phase, or the list of control entity identifiers supported by a AN is changed, e.g. the optional control entity Change Count TLV (control entity Change Count TLV is described in the IEEE Std 802.16) obtained from the network as part of obtaining the control entity ID list, is different with that stored in the configuration information of the STA, the STA SHOULD get the list from the network. Otherwise, available control entity(s) associated with a AN SHOULD be enumerated locally based on the configuration information of the STA.

### Control Entity Enumeration and Selection

For automatic selection, an STA makes its control entity selection decision based on the dynamic information obtained within a coverage area (e.g., a list of available control entity Identifiers offering services), and configuration information. The specific algorithms that an STA MAY use to select the most preferred control entity from the list of discovered control entities are out of scope of this release.

For manual selection, the user manually selects the most preferred control entity based on the dynamic information obtained within the coverage area. Manual selection can also enable use scenarios where a non-subscribed user wants to connect to a detected network. For example, the user wants to exercise an initial provisioning procedure with a specific control entity, or it wants to use the network on “pay for use” basis.

### ASN Attachment Based on Control Entity Selection

Following a decision to select a particular control entity, an STA SHOULD indicate its control entity selection by attaching to an ASN associated with the selected control entity, and by providing its identity and home control entity domain in the form of NAI. The AN SHOULD use the realm portion of the NAI to determine the next AAA hop to where the STA’s AAA packets SHOULD be routed. The STA SHOULD use its NAI with additional information (also known as decorated NAI) to influence the routing of the next AAA hop when the home control entity realm is only reachable via another mediating realm (e.g., a visited control entity).