|  |
| --- |
| Examples for the tenets in IEEE 802.1CF |
| Date: 2014-01-20 |
| **Authors:** |
| Name  | Affiliation  | Phone  | Email  |
| Max 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

This documents provides example text for the tenets section in the IEEE 802.1CF. The presented text is provided for information only and is not aimed for adoption in the recommended practice without excluding that some of the statements will later appear in the specification.

The text proposal is derived from the tenets section of the WiMAX Forum NWG Stage 2 document adapted to the particular scope of the IEEE 802.1CF specification.

Tenets for Network Reference Model and Functional Description of IEEE 802 Access Network

The tenets presented in this section were taken into account for the development of the Recommended Practice.

## General

1. The IEEE 802 Access Network SHOULD be based on the existing IEEE 802 standards and their amendments. In the event that currently defined IEEE 802 protocols do not satisfy a solution requirement, extensions MAY be proposed.
2. The IEEE 802 Access Network solution SHOULD employ use of native IEEE 802.1 procedures and logical separation between such IEEE procedures and IP-layer addressing, routing and connectivity management procedures and protocols to enable use of the access architecture primitives in standalone and interworking deployment scenarios.
3. The Network Reference Model and Functional Description framework SHOULD be based on functional decomposition principles (i.e. decomposition of features into functional entities across interoperability reference points, without specific implementation assumptions including the notion of network entities and interfaces). Such a framework SHOULD be modular and flexible enough to accommodate a broad range of deployment options such as:
* Small-scale to large-scale (sparse to dense connectivity coverage and capacity) networks,
* Hierarchical, flat, or mesh topologies, and their variants,
* Co-existence of fixed, nomadic, portable and mobile usage models.
1. The solution MAY be flexible so it is likely that it accommodates future enhancements to the IEEE 802 suite of standards.

## Network Reference Model

1. The architecture framework SHOULD permit decoupling of IEEE 802 based access architecture (and supported topologies) from connectivity IP services and SHOULD consider network elements of the IP connectivity network agnostic to the IEEE 802 Access Network.
2. The architecture SHOULD be agnostic to and support access to a variety of independent application service providers.

## Access Network Control Architecture

1. The architecture SHOULD support sharing of an IEEE 802 access network by multiple service providers.
2. The architecture SHOULD support that a single service provider offers service over multiple IEEE 802 Access Network – managed by one or more access operators.
3. The architecture SHOULD support access providers that employ one or more IEEE 802 Access Network topologies.
4. The architecture SHOULD specify open, published and accepted standards based and well-defined reference points between the station and the IEEE 802 Access Network, between the station and the control entity, between the IEEE 802 Access Network and the control entity, as well as between IEEE 802 Access Networks controlled by the same control entity.
5. The architecture MAY support evolution paths between the various usage models subject to reasonable technical assumptions and constraints.
6. The architecture SHOULD support the most trivial scenario of a single operator deploying an IEEE 802 Access Network together with a limited set of control functions, so that the operator can offer basic service access without consideration for roaming or interworking with other service providers.
7. The architecture SHOULD enable IEEE 802 Access Network and control entity system designs that easily scale upward and downward – in terms of coverage, range or capacity.
8. The architecture SHOULD accommodate a variety of transport links, both wireline and wireless with different latency and throughput characteristics.
9. The architecture SHOULD support incremental infrastructure deployment.

## Network Discovery and Selection

1. The architecture SHOULD support the discovery and selection of accessible service providers by a station.
2. The IEEE 802 Access Network architecture SHOULD enable a user to manually or automatically select from available service providers.
3. The architecture MAY be able to accommodate documented geo-specific constraints.

## Association, Disassociation

1. The solution SHOULD support the integration of access network access entities (base stations, access points) of varying technologies, coverage and capacity – for example, pico, micro, and macro base stations/access points of different IEEE 802 technologies.

## Authentication and security

1. The solution SHOULD accommodate support for strong mutual station authentication between a station and the IEEE 802 Access Network, based on the IEEE 802.1X security framework.
2. The solution SHOULD support a variety of user authentication credential formats such as username/password, digital certificates and Subscriber Identity Module (SIM).
3. A station MAY be able to support all commonly deployed authentication mechanisms and authentication in home and visited operator network scenarios based on a consistent and extensible authentication framework.
4. The solution SHOULD support data integrity, replay protection, confidentiality and non-repudiation using applicable key lengths within the IEEE 802 Access Network.
5. The IEEE 802 Access Network security framework SHOULD be agnostic to the operator type and access network topology.

## Service, QoS and Policy control

1. The solution SHOULD support inter-operator policy definition, distribution and enforcement as needed for different kind of communications. The following capabilities SHOULD apply (subject to specific services offered and provisioned):
* The architecture SHOULD support SLA-based resource management for subscribers,
* The architecture SHOULD support simultaneous data sessions,
* The architecture SHOULD support prioritization (including pre-emption) for high priority sessions.
1. The solution SHOULD support the means to implement policies as defined by various operators for QoS based on their SLAs, which MAY require policy enforcement per user and user group as well as factors such as location, time of day, etc.
2. QoS policies MAY be synchronized between operators depending on subscriber SLAs, accommodating for the fact that not all operators MAY implement the same policies.
3. The solution SHOULD use standard IEEE 802 mechanisms for managing policy definition and policy enforcement between operators.

## Datapath establishment, relocation and teardown

1. The solution SHOULD NOT preclude inter-access technology handovers, when such capability is enabled in multi-mode station.
2. The solution SHOULD NOT preclude roaming between different service providers.
3. The solution SHOULD support mechanisms to support seamless handovers at up to modest speeds.
4. The solution SHOULD support the relocation management requirements associated with the fixed, nomadic, and mobile usage scenarios such as the mobility restriction of fixed and nomadic users.

## Accounting

1. The solution SHOULD support the accounting requirements for all usage scenarios without dependencies on particular network configurations.