|  |
| --- |
| Chapter 6.9.4 Public hotspot |
| Date: 2017-03-08 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Max Riegel | Nokia Bell Labs |  | maximilian.riegel@nokia.com |
|  |  |  |  |
|  |  |  |  |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG 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 document proposes content for description of the public hotspot deployment scenario.

# Functional Decomposition and Design

## Deployment scenarios

### Public hotspot

Public hotspots deploy IEEE 802 access networks similar to enterprise networks, and usually provide access to the Internet only over a wireless LAN. Public hotspots can widely vary in size and capabilities; however, they have a defined set of commonalities to ensure, that customers find access regardless of the particular implementation.

They all provide at least an open WLAN and block access to the Internet until the user opened a captive portal page and confirmed the terms and conditions often combined with the entry of credentials, which the hotspot operator could use for identification of the user and for charging for the service. More capable hotspots provide in addition possibilities for fully automatic login, sometimes through proprietary solutions based either on detecting the MAC addresses of the terminals or based on credentials temporary established in the web-browser used for accessing the captive portal page. Aside of proprietary solutions for automatic access to open WLANs, standardized solutions exist for access to secured WLANs based on 802.1X authentication and provisioning of credentials. The credentials can be made available at the terminal either through prior establishment of a permanent subscription with the hotspot operator or one of its roaming partners, or through an online signup process at the hotspot according to the Hotspot 2.0 procedures.

Virtual LAN capabilities in the IEEE 802 technologies allow to configure both kinds of public hotspots within the same network infrastructure. A hotspot usually consists of a number of WLAN access points connected through an Ethernet switch to an access gateway, which contains the mechanisms of the captive portal and provides the access router with NAT and firewall for the IP connectivity of the terminals to the Internet.



Figure x: Public hotspot network scenario

As visible in the figure x above, commercial hotspots usually deploy a WLAN controller to establish a more consistent and seamless service across the whole coverage area. They have a network management station in place to facilitate efficient configuration and management of the infrastructure, and they deploy an evolved authentication center, which can establish and maintain a bigger number of temporary user accounts. The authentication center is also responsible for the communication with roaming partners, technically spoken, it contains the RADIUS proxy for forwarding authentication requests to the home service provider.

Like the enterprise network, the public hotspot network can be well mapped to the NRM. The backhaul is represented by the Ethernet switch, WLAN access points are building the nodes of attachment. The functions of the WLAN controller fit well to the role of the ANC, and network management station and the authentication center well map to NMS and SS, respectively.



Figure x+: Mapping of the hotspot network to the NRM

Many of the reference points of the NRM map to interfaces of the public hotspot network. All reference points towards terminals are supported. R6 is exposed on the interface between the switch and the access point, and R3 maps to the LAN cable between the switch and the router in the access gateway. Also the majority of the control interfaces of the access network are present in the public hotspot network. R5 can be mapped to the communication between the WLAN controller and the WLAN access points, and R4 and R11 denote the protocol connections between the WLAN controller and the authentication center and network management station, respectively. The information exchanges between the authentication center and the access gateway to temporarily open access to the Internet for users can be mapped to the R12 reference point.

However, not all reference points are such clearly exposed in public hotspot networks. R7 and R9 may exist, but related ANC functions may be implemented in the Ethernet switch in the backhaul. Aside of solutions, which closely follow the functional decomposition represented by the NRM, there exist equipment for public hotspots, which integrates and combines functions of a public hotspot into a single device to make installation and operation easier. E.g. a favorable solution for smaller public hotspot may be a device, which integrates the WLAN controller, the Ethernet switch and the access gateway with captive portal into a single box.