|  |  |  |  |
| --- | --- | --- | --- |
| P802.1CF/D2.2 CID-30+33 comment resolution proposal | | | |
| Date: 2018-09-24 | | | |
| **Authors:** | | | |
| Name | Affiliation | Phone | Email |
| Max Riegel | Nokia |  | 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 provides text amendment proposals to address comments i-30 and i-33 of the initial sponsor ballot on P802.1CF-D2.2

# Text amendment to address i-30 (James) + i-33 (Brian):

* Virtualized WLAN access network for in-building IoT services

In-building IoT services provided by utilities and other companies benefit from virtualized WLAN access infrastructures dedicated to IoT services. These IoT services are built around a client-server architecture consisting of a high number of small, inexpensive client devices connected to a central server interacting with the distributed devices and operating the higher layer control and data-processing functions of IoT services. Due to its ubiquitous availability and the availability of a vast number of low-cost chipset solutions, WLAN has become the network interface of choice for that kind of IoT service deployments.

Putting IoT devices on a WLAN network aimed for office or residential use, however, imposes a number of risks and drawbacks. IoT devices are usually kept in operation for much longer periods than smartphones, tablets, and notebook computers, and often completely miss the regular software updates that are usual for the much more powerful and complex handheld communication devices. It is quite common that IoT devices are intended to run for more than a decade, completely without maintenance, serving their very specialized purpose. Due to limited configuration and management capabilities, it is quite likely that vulnerabilities in the communication software and operating system detected during the lifetime of an IoT device will not be fixed through a firmware update. Missing agents in the legacy devices make it difficult for network administrators to remotely manage these devices. Keeping such devices in a LAN together with other systems and arbitrary access to the Internet allows not only malicious attacks to the IoT devices by leveraging unpatched vulnerabilities, but also the misuse of the IoT devices to attack other devices in the same access network as well as perform distributed denial of service attacks to any location in the Internet.

In addition to the security risks, there are also performance impacts introduced by operating potentially aged, simple, low-cost IoT devices together with the most recent smartphones, tablets, and other computing devices on a single WLAN access network. Even when the most recent WLAN is still backward compatible with the legacy IEEE 802.11b standard, attaching legacy WLAN equipment to a modern WLAN access network requires the activation of backward-compatibility modes, which lowers the efficiency of the complete WLAN access network.

Both the security and the efficiency challenges can be mitigated by setting up a dedicated WLAN access network for IoT devices. Keeping lower performance IoT devices in a separate network allows for optimizations of the network configurations to their native purpose—e.g., enabling legacy backward-compatibility modes in the radio interfaces only when there is real need for them. Specific filtering rules could be applied to IoT devices limiting broadcasting inside the access network to prevent vulnerable devices from attacking other devices in the network or connecting to any host in the Internet. The IoT devices still use Internet protocols for communication, but their communications are restricted within a virtual private network to mitigate the risks of the public Internet.

Network virtualization allows for establishment of multiple independent access networks on a common infrastructure and is well supported by IEEE 802 technologies through inherent support of virtualization.

* Virtualized WLAN access for IoT

Figure 25 shows how a virtualized WLAN access network for in-building IoT could be realized by leveraging the fixed broadband access infrastructure over either cable, DSL, or fiber providing broadband Internet access to homes. Core functionality of the solution is the establishment of the virtualized NA in the homes by setting up a second AP instance on the WLAN interface of the residential customer-premises equipment (CPE). To establish the desired isolation of the WLAN access network for IoT devices, the second AP instances in the CPEs have to be attached to a separate control plane to allow for the desired security and access control by the IoT service provider. A separate datapath for the second WLAN forwards all the traffic going over the IoT WLAN to the IoT service provider and prevents IoT devices from establishing uncontrolled connections to the Internet with the inherent risk of getting compromised through those connections. Remote CPE management, e.g. supported by TR-069 CPE WAN management protocol and TR-181 device information model, can be used by the Internet service provider to remotely configure the second AP instance, second datapath, and second control entities within the CPE. It also allows to remotely reapply the same configurations, when the CPE is replaced through newer hardware, which can happen during the long lifetime of IoT applications.

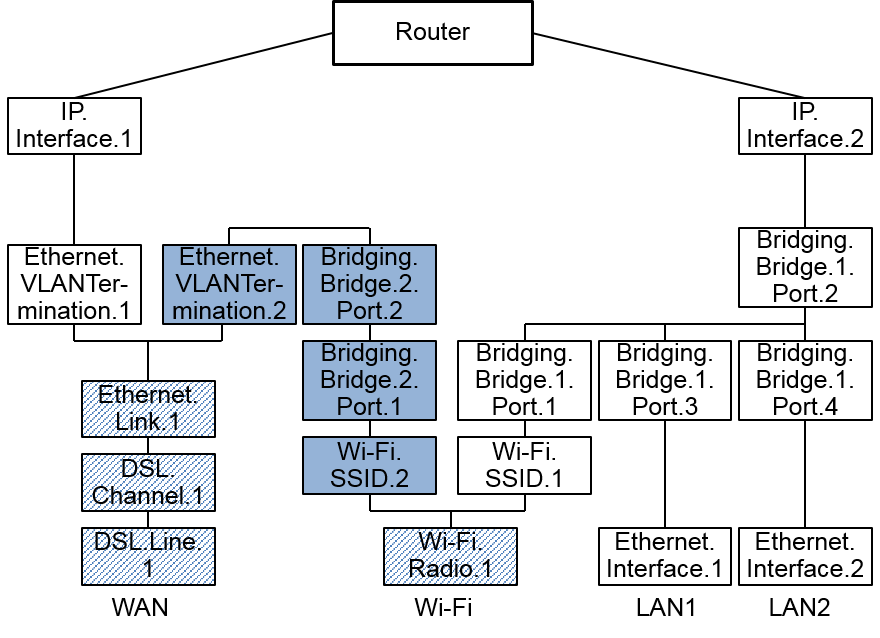


Figure 25+1 – Schematic datapath and WLAN configuration model of CPE with IoT WLAN

Figure 25+1 shows in a schematic diagram the additional configuration elements needed to establish the IoT WLAN and the second datapath for in-building IoT services within a remotely managed CPE.

In the broadband access infrastructure the second datapath and control plane for the IoT WLAN AP instances are established by the Internet service provider and provided to the IoT service provider as a kind of “WLAN as a Service.” After instantiation of the second WLAN access network, the IoT service provider can control and operate the virtualized WLAN access network for IoT devices like a dedicated network. It has its own operation, administration, and maintenance through a separate NMS, enabling independent access to all management data belonging to the virtualized WLAN access network. Only a few PHY-related configurations like radio channel assignments of the WLAN APs can’t be independently configured by the IoT service provider but are preset by the owner of the infrastructure.

While the description in the previous paragraphs shows the realization of a virtualized WLAN access network in the residential broadband access network, the same kind of virtualized WLAN access for IoT devices could also be realized in enterprise WLAN access networks. The example of the enterprise network with multiple independent bridging domains and multiple SSIDs enabled on the WLAN APs introduced in Clause 5.9.4 shows the establishment of separate datapaths for separating traffic and connectivity with a common control plane and a common network management system. Applying virtualization to the control entities and to the network management system of enterprise networks would facilitate the establishment of a dedicated WLAN for IoT devices under the control of a different entity.

Such virtualized WLAN access infrastructure can be well represented and described through the Network Reference Model, the functional description, and the information models provided by this specification. The presented deployment case provides an example of the IEEE 802 access network virtualization introduced in Clause 5.8.

In Figure 26, the mapping of the usage scenario of virtualized WLAN access network for in-building IoT services to the NRM is depicted. The NRM instance in front represents the Internet access network for residential use. The NRM instance in the back represents the virtualized WLAN access for IoT devices under the operational control of the IoT service provider. For each of the WLANs, an access network with its own control and NMS is established. A common CIS allows the two network instances to coordinate their operation and align network resource allocations. NMS as well as SS of the NRM instance in the back belong to the IoT service provider with data directly forwarded over R3 of the access network to the dedicated AR belonging to the IoT service provider.



* Mapping of virtual WLAN access for IoT devices to NRM

Figure 26 does not expose details of shared components of the two separate WLAN access networks. In principle there would be three different roles in the deployment scenario: the entity owning and operating the physical broadband access infrastructure and managing the residential CPEs, the IoT service provider operating and controlling WLAN access for IoT devices, and the Internet service provider operating the residential broadband Internet connectivity. In many cases, the entity owning and operating the physical access infrastructure might be combined with the entity providing the residential Internet access. However, it would also be feasible that operation of the physical access infrastructure would be completely separate to the service providers based on virtualized WLAN access networks on a shared infrastructure. Furthermore, IEEE 802 technologies are not limited to two instances of virtualized access networks, but would allow for more instances enabling further businesses to establish their own network operations.