CAPWAP Working Group
Internet Draft
Document: Objectives for Control and Provisioning of Wireless Access Points
Expires: April 2005

Wenhui Zhou
China Mobile Communication Corporation
Zhonghui Yao
Huawei Technologies
Lily Yang
Intel Corp.
Meimei Dang
Research Institute of Telecommunication Transmission
Dong Wang
ZTE

November 2004

Objectives for Control and Provisioning of Wireless Access Points (CAPWAP) Protocol

draft-zhou-capwap-objectives-00.txt

Status of this Memo

Abstract

This document presents a set of objectives or requirements for the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. It presents the requirements from different aspects including architecture, user (client) access, service, control, management and security.

1. Definitions

1.1 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

1.2 Terminology Used in this Document

CAPWAP - Control and Provisioning of Wireless Access Points.

CAPWAP Functions - a set of WLAN control functions that are not directly defined by IEEE 802.11 Standards, but deemed essential for effective control, configuration and management of 802.11 WLAN access networks.

Wireless Termination Point (WTP) - the physical or network entity that contains RF antenna and 802.11 PHY to transmit and receive station traffics for the IEEE 802.11 WLAN access networks. Such physical entities are often called "Access Points" (AP) previously, but "AP" can also be used to refer to logical entity that implements 802.11services. So we recommend using "WTP" instead to explicitly refer to the physical entity.

Centralized WLAN Architecture - the WLAN access network architecture family in which the logical functions, including both IEEE 802.11 and CAPWAP functions (wherever applicable), are implemented across a hierarchy of network entities. At the low level of such hierarchy are the WTPs while at the higher level are the Access Controllers(ACs), which are responsible to control, configure and manage the entire WLAN access networks.

Access Controller (AC) - The network entity in the Centralized WLAN architectures that provide WTPs access to the centralized hierarchical network infrastructure, either in the data plane, control plane, or management plane, or a combination therein.

Local MAC Architecture - A sub-group of the Centralized WLAN Architecture, where the majority or entire set of 802.11 MAC functions (including most of the 802.11 management frame processing) are implemented at the WTP. Therefore, the 802.11 MAC stays intact and local in the WTP, along with PHY.

Split MAC Architecture - A sub-group of the Centralized WLAN Architecture, with the characteristic that WTPs in such WLAN access networks only implement the delay sensitive MAC services (including all control frames and some management frames) for IEEE 802.11, while tunneling all the remaining management and data frames to AC for centralized processing.The IEEE 802.11 MAC as defined by IEEE 802.11 Standards is effectively split between the WTP and AC.

2. Introduction

As IEEE 802.11 Wireless LAN (WLAN) technology matures, large scale deployment of WLAN networks is highlighting certain technical challenges including management, monitoring and control of large number of Access Points (APs). Distributing and maintaining a consistent configuration throughout the entire set of APs in the WLAN is a difficult task. The shared and dynamic nature of the wireless medium also demands effective coordination among the APs to minimize radio interference and maximize network performance. Furthermore, vendors implement not only the services defined in the IEEE 802.11 standard, but also a variety of value-added services or functions, like load balancing support, QoS, station mobility support, rogue AP detection, etc.

The Centralized WLAN Architecture family, as described in [2], is an innovative architectural solution intended to address the aforementioned problems. Two classes of the Centralized WLAN Architecture family, namely the Local MAC and the Split MAC, will be supported by the CAPWAP protocol to realize interoperability of the AC-WTP interface among vendors. This document puts forth the requirements for CAPWAP protocol between the AC and WTP.

2.1 Centralized WLAN Architecture

Figure 1 shows a diagram of the Centralized WLAN Architecture from [2]. In the Centralized WLAN Architecture, there is one or more centralized controllers for managing a large number of WTP devices. The centralized controller is commonly referred to as an Access Controller (AC), whose main function is to manage, control and configure the WTP devices that are present in the network. In addition to being a centralized entity for the control and management plane, it may also become a natural aggregation point for the data plane, since it is typically situated in a centralized location in the wireless access network. The AC is often co-located with an L2 bridge, a switch, or an L3 router, and hence may be referred to as Access Bridge, or Access Router in those particular cases. Therefore, an Access Controller could be either an L3 or L2 device, and Access Controller is the generic terminology we use throughout this document.

It is also possible that multiple ACs are present in a network for purposes of redundancy, load balancing, etc. This architecture family has several distinct characteristics that are worth noting. First of all, the hierarchical architecture and the centralized AC afford much better manageability for the large scale networks. Secondly, since the IEEE 802.11 functions and the CAPWAP control functions are provided by the WTP devices and the AC together, the WTP devices themselves may not implement the full 802.11 functions as defined in the standards any more. Therefore, it can be said that the full 802.11 functions are implemented across multiple physical network devices, namely, the WTPs and ACs. Since the WTP devices only implement a portion of the functions that standalone APs implement, WTP devices in this architecture are sometimes referred to as light weight or thin APs by some vendors.

As shown in Figure 1, CAPWAP protocol is the protocol between WTP and AC that will provide vendor interoperability when it is standardized. This protocol may run on different interconnection technology.

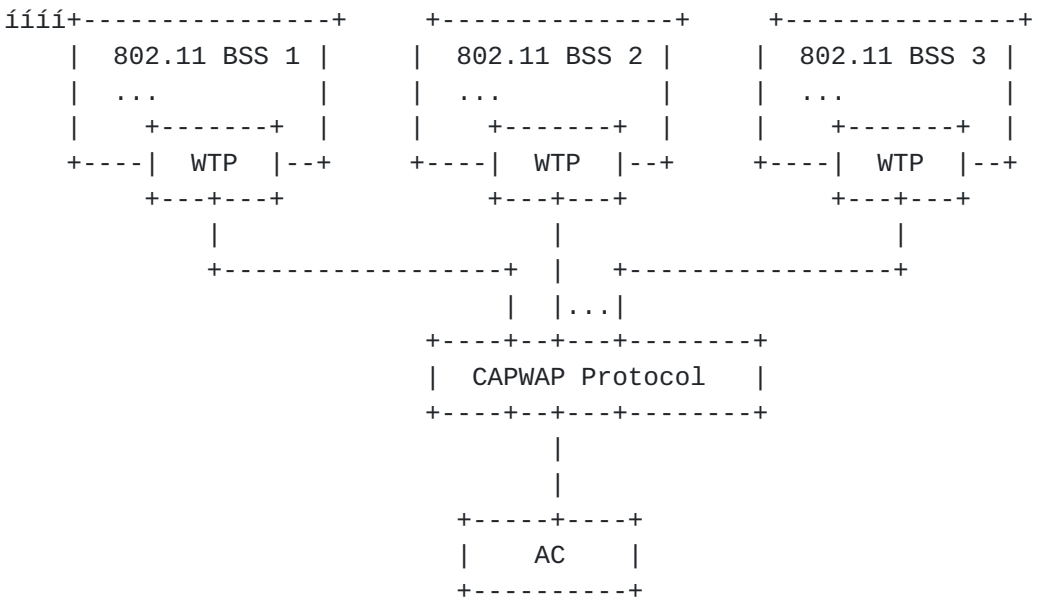

Figure 1: Centralized WLAN Architecture Diagram

2.2 Local MAC

The main motivation of Local MAC architecture model is to offload network access policies and management functions (CAPWAP functions described in [2]) to the AC, without splitting the 802.11 MAC functionality between WTPs and AC. The whole 802.11 MAC resides on the WTPs locally, including all the 802.11 management and control frame processing for the STAs; on the other hand, information related to management and configuration of the WTP devices is communicated

with a centralized AC, to facilitate management of the network, and maintain a consistent network-wide configuration for the WTP devices.

2.3 Split MAC

The main idea behind the Split MAC architecture is to implement part of the 802.11 MAC functionality on a centralized AC instead of the WTPs, in addition to the services required for managing and monitoring the WTP devices. Usually, the decision of which functions of the 802.11 MAC need to be provided by the AC is based on the time-criticality of the services considered.

In the Split MAC architecture, the WTP terminates the infrastructure side of the wireless physical link, provides radio-related management, and also implements all time-critical

functionality of the 802.11 MAC. In addition, the non real-time management functions are handled by a centralized AC, along with higher-level services, such as configuration, QoS, policies for load-balancing, access control lists, etc. The subtle but key distinction between Local MAC and Split MAC relates to the non real-time functions: in Split MAC architecture, the AC terminates 802.11 non real-time functions, whereas in Local MAC architecture the WTP terminates the 802.11 non real-time functions and consequently sends appropriate messages to the AC.

There are several motivations for taking the Split MAC approach. The first is to offload to the WTP functionality that is specific and relevant only to the locality of each BSS, in order to allow the AC to scale to a large number of 'light weight' WTP devices. Moreover, real-time functionality is subject to latency constraints and cannot tolerate delays due to transmission of 802.11 Control frames (or other real-time information) over multiple-hops. The latter would limit the available choices for the connectivity between the AC and the WTP, hence the real-time criterion is usually employed to separate MAC services between the devices. Another consideration is cost reduction of the WTP to make it as cheap and simple as possible. Last but not least, moving functions like encryption and decryption to the AC reduces vulnerabilities from a compromised WTP, since user encryption keys no longer reside on the WTP. As a result, any advancements in security protocols and algorithms design do not necessarily obsolete the WTPs; the ACs implement the new security schemes instead, and the management and update task is therefore simplified. Additionally, the network is protected against LAN-side eavesdropping.

3. Architectural requirements

The following are the architectural requirements for CAPWAP protocol:

1) Both local MAC and split MAC technologies based products, i.e., ACs or WTPs must be able to co-exist and inter-operate in one WLAN access network.

2) ACs and WTPs MUST be able to connect by a variety of interconnect technologies. CAPWAP protocol should be transmitted transparently regardless of lower technologies. Examples of interconnect technologies used in current architectures include Ethernet, bus backplanes, and ATM (cell) fabrics. Ethernet architecture is most widely used and should be recommended.

3) CAPWAP-supported WTPs should be able to co-exist with non-CAPWAP WTPs in one WLAN access network.

4. User (client) access requirements

There shouldn't be any impact on the client (both hardware and software platform) due to the use of CAPWAP protocol. Clients should not be required to be aware of the existence of CAPWAP protocol.

5. Service requirements

The following are the service requirements:

1)Voice over WLAN. So CAPWAP should support IEEE 802.11e and provide fast-handoff capability to avoid voice interruption.

2)Isolate STA from other STAs and restrict inter-STA in layer 2 communication directly.

3)WLAN network resource share. It is required that two or more WLAN service providers can share a hotspot WLAN network. This means that a physical WLAN network can be virtualized into several logical WLAN network.

6. Centralized Control requirements

The following are the control requirements:

1)AC may perform access control functions based on radio resource and/or network resource.

2)To support handover and load balancing between different WTPS, AC should have the capability of centralized control via CAPWAP protocol.

7. Management Requirements

The following are the management requirements:
It is possible that WTPs can be managed directly or through AC where AC acts as a management agent.

8. Security Requirements

The following are the security requirements:

1)It is required to support WPA and/or IEEE 802.11i for wireless air interface security.

2)It is required to provide mechanism supporting secure information exchange between AC and WTP

9. QoS Requirements

The following are the QoS requirements:

WLAN air interface QoS implementation should be based on the current IEEE802.11e, but it is required to support QoS centralized control Policy between WTPS and AC via CAPWAP protocol.

10. References

1. í CAPWAP Problem Statementí , August 2004, <http://www.ietf.org/internet-drafts/draft-ietf-capwap-problem-statement-02.txt>

2. í Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)í , August 2004, http://www.ietf.org/internet-drafts/draft-ietf-capwap-arch-05.txt>

3. í Functionality Classifications for Control and Provisioning of Wireless Access Points (CAPWAP)í , July 2004, <http://www.ietf.org/internet-drafts/draft-cheng-capwap-classifications-01.txt>

11. Authors' Addresses

Wenhui Zhou
53A, Xibianmen Ave, Xuanwu District
Beijing 100053
P. R. China
Phone: +86 10 66006688 ext.3061
Email: zhouwenhui@chinamobile.com

Zhonghui Yao
Huawei Longgang Production Base,
Shenzhen 518129
P. R. China
Phone: +86 755 28780808
EMail: yaoth@huawei.com

L. Lily Yang
JF3-206, Intel Corp.
2111 NE 25th Ave.
Hillsboro, OR 97124
USA
Phone: +1 503 264 8813
EMail: lily.l.yang@intel.com

Meimei Dang
RITT,CATR
No.11 YueTanNanJie, Xicheng District
Beijing 100045
P.R.China
Phone: +86 10 68094457
Email: dangmeimei@mail.ritt.com.cn

Dong Wang
No.68 Zijinghua Rd,Yuhuatai District,
Nanjing,Jiangsu Prov. 210012
P.R. China.
Phone: +86-25-52871713
EMail: wang.dong@mail.zte.com.cn

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.