CAPWAP Working Group
Internet-Draft
Expires: May 2005

S. Govindan (Editor)
Panasonic
ZH. Yao
Huawei
WH. Zhou
China Mobile
L. Yang
Intel
H. Cheng
Panasonic

November 2004

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

draft-ietf-capwap-objectives-00.txt

Status of this Memo

Copyright Notice

Abstract

This document presents a set of objectives for an interoperable protocol for the Control and Provisioning of Wireless Access Points (CAPWAP). It presents objectives in three categories: architecture, operations and security. The primary purpose of the document is to present focused requirements which when realized, will ensure interoperability among wireless local area network (WLAN) devices of alternative designs. These objectives will form the basis for the development and evaluation of a CAPWAP protocol.

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Terminology

This document follows the terminologies of [I-D.ietf-capwap-arch]. Additionally, the following terms are defined;

Switching segment: Those aspects of a centralized WLAN that primarily deal with switching or routing control and data information between Wireless Termination Points (WTPs) and the WLAN controller.

Wireless medium segment: Those aspects of a centralized WLAN that primarily deal with the end-user interface which is wireless. Initially, CAPWAP focuses on IEEE 802.11 technologies but this segment may also refer to other technologies such as IEEE 802.16.

CAPWAP framework: A term that includes the local MAC and split MAC designs of the Centralized WLAN Architecture. Standardization efforts are focussed on these designs.

CAPWAP protocol: The protocol between WLAN controller and WTPs in the CAPWAP framework. It facilitates control, management and provisioning of WTPs in an interoperable manner.

3. Introduction

The growth in large scale wireless local area network (WLAN) deployments has brought to focus a number of technical challenges. This includes the complexity of managing large numbers of wireless termination points (WTPs), which is further exacerbated by differences in their design. Another challenge is the maintenance of consistent configurations among the numerous WTPs. The dynamic nature of the wireless medium is also a concern together with WLAN security. These challenges have been highlighted in [I-D.ietf-capwap-problem-statement].

Many vendors have addressed these challenges for large scale WLAN deployments by developing new architectures and solutions. A survey of the various architectures and solutions was conducted to better understand the context of the challenges so as to develop interoperability among them. The Architecture Taxonomy [I-D.ietf-capwap-arch] is a result of this survey in which major architecture families are classified. Broadly, these are the autonomous, centralized WLAN and distributed mesh architectures. The survey showed that the current majority of large scale deployments follow the centralized WLAN architecture in which portions of the wireless medium access control (MAC) operations are centralized in a WLAN controller. This architecture family is further classified into remote MAC, split MAC and local MAC. Each differs in the degree of separation of MAC layer capabilities among WTPs and WLAN controller.

This document puts forth critical objectives for achieving interoperability in a CAPWAP framework. It presents objectives that address the challenges of large scale WLAN deployments. The realization of these objectives will ensure that WLAN equipment of major design types may be integrally deployed and managed.

4. Categories of Objectives

The objectives for the CAPWAP protocol are organized into three major categories; architecture, operations and security.

Architecture objectives deal with system level aspects of the CAPWAP protocol. They address issues of protocol extensibility, diverse network deployments and architecture designs and differences in transport technologies.

Operational objectives address the control and management features of the CAPWAP protocol. They deal with operations relating to system-wide resource management, WTP management, QoS and STA access control.

Security objectives address potential threats to WLANs and their containment. Specifically, they deal with securing the CAPWAP protocol and the WLAN system as a whole. The objectives also address security requirements from end-users and service providers.

5. Architecture Objectives

The architectural considerations of centralized WLAN networks are fundamental to the development and evaluation of a CAPWAP protocol. The objectives in this category deal with system level aspects relating to protocol extensibility, diversity of network deployments and differences among vendor equipment.

5.1 Interoperability Objective

Two major designs of the centralized WLAN architecture are local MAC and split MAC. With the focusing of standardization efforts on these two designs, it is crucial to ensure mutual interoperation among them.

5.1.1 Objective Details

This objective for the CAPWAP protocol is to ensure that WTPs of both local MAC and split MAC architecture designs are capable of interoperation within a single WLAN. Consequently, a single WLAN controller will be capable of controlling both types of WTPs using a single CAPWAP protocol. Integral support for these designs comprises a number of protocol aspects.

i. Functionality negotiations between WLAN controller and WTPs

Local MAC and split MAC designs differ in the degree of IEEE 802.11 MAC functionalities that each type of WTP realizes. The CAPWAP protocol should allow WLAN controllers to determine the functionalities of different WTPs as a first step in controlling them.

ii. Establishment of alternative interfaces

The functionality differences among different WTPs essentially equates to alternative interfaces with a WLAN controller. So the CAPWAP protocol should be capable of adapting its operations to the different interfaces. The definition of these interfaces is dependent on the functionality differences among local MAC and split MAC WTPs. It is therefore out of scope of the objectives specifications.

[Functionality Classifications] presents additional details on these two aspects. It shows how flexibility in the CAPWAP protocol may be achieved so as to realize this architecture objective.

This objective also addresses the need for flexibly configuring WTPs based on their design types and other setup aspects.

5.1.2 Motivation and Protocol Benefits

The benefits of realizing this architecture objective are both technical and practical. First, there are substantial overlaps in the control operations of local MAC and split MAC architecture designs. As a result, it is technically practical to devise a single protocol that manages both types of devices.

Next, the ability to operate a CAPWAP protocol for both types of architectural designs enhances its practical prospects as it will have wider appeal.

Furthermore, the additional complexity resulting from such alternative interfaces is marginal. Consequently, the benefits of this objective will far outweigh any cost of realizing it.

5.1.3 Relation to Problem Statement

The objective for supporting both local MAC and split MAC WTPs is fundamental to addressing [I-D.ietf-capwap-problem-statement]. It forms the basis for those problems to be uniformly addressed across the major WLAN architectures. This is the ultimate aim of standardization efforts. The realization of this objective will ensure the development of a comprehensive set of solutions to the challenges of large scale WLAN deployments.

5.1.4 Customer Requirements

A number of service providers and equipment vendors see benefits with the combined usage of both local MAC and split MAC designs. WTPs of different designs are placed in different locations so as to selectively take advantage of their respective characteristics. The integral support of different architectures therefore addresses critical needs for the market.

Furthermore, since there are products of each design type already in the market and widely deployed, it is necessary for CAPWAP protocol to support both of them.

5.1.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

5.2 Interconnection Objective

Large scale WLAN deployments are likely to use a variety of interconnection technologies between different devices of the

network. It should therefore be possible for the CAPWAP protocol to operate over the different interconnection technologies. So the protocol needs to be independent of underlying transport technologies.

5.2.1 Objective Details

WLAN controllers and WTPs must be able to connect by a variety of interconnection technologies. The fundamental intent is for CAPWAP protocol exchanges to be transparent to underlying transport technologies. As a result of realizing this objective, the protocol will be capable of operation over different interconnect technologies including Ethernet, bus backplanes, ATM (cell) fabrics and also wireless technologies such as IEEE 802.11. Ethernet architecture is most widely used and should be recommended.

The CAPWAP protocol should have the ability to support this diversity of interconnection technologies for data and control exchanges. For example, VLAN tunnels are an example of an interconnection technology over which CAPWAP may operate.

Related to this objective, is the QoS aspect of interconnection technologies. Given that QoS will be enabled differently in each of these technologies, the CAPWAP protocol must ensure that network performance is consistent across different transport means. Additionally, QoS consistency has to cover the switching segment and the wireless medium segment.

5.2.2 Motivation and Protocol Benefits

[TBD]

5.2.3 Relation to Problem Statement

[TBD]

5.2.4 Customer Requirements

[TBD]

5.2.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

5.3 Support for Logical Networks

Large WLAN deployments are complex and expensive. Furthermore,

enterprises are under pressure to improve the efficiency of their expenditures. These issues are increasingly being addressed by means of shared deployments. As a result, a number of logical networks cover a single physical WLAN infrastructure. This way the cost of deployment and management can be shared among network service providers. A scenario together with additional details for such shared WLANs is presented in [Functionality Classifications].

5.3.1 Objective Details

The objective for supporting logical networks involves a number of aspects. These are discussed below;

i. WLAN management in terms of logical groups

Traditionally, each WTP has represented one complete subset of a larger WLAN system. However, with shared deployments, each WTP represents a number of subsets of possibly a number of larger WLAN systems. So with such deployments, WLANs need to be managed in terms of logical groups instead of physical devices.

ii. Mutual separation of control and communications

Since different logical networks are likely to be associated to different enterprises, it is crucial that control and data communications among them be mutually separated. In addition to being a security concern, this aspect of the objective also highlights a complexity concern. Specifically, mixing of traffic for different logical networks can complicate control. So the CAPWAP protocol must be capable of separating traffic among logical networks. VLANs and other types of tunnels may be used for this purpose.

iii. Multiple authentication mechanisms

The presence of multiple logical networks within an infrastructure also means there are different subscriber groups in a WLAN system. Since the subscriber groups are likely to belong to different service providers or WLAN domains, their authentication needs will also be different. As a result, the CAPWAP protocol must be capable of transferring different authentication information. For example, one subscriber group may be authenticated with IEEE 802.11i with the WLAN controller being the authenticator, while another group could use web authentication at an alternative server.

5.3.2 Motivation and Protocol Benefits

Given the realities of cost and complexity of WLANs, a CAPWAP

protocol that incorporates the objective of supporting logical networks ensures simpler and cost effective WLAN management and deployment. A protocol that realizes this is therefore consistent with the goal of reducing complexity in large scale WLANs.

5.3.3 Relation to Problem Statement

This objective for supporting logical networks addresses problem of management complexity in terms of cost. Such cost complexity is reduced by sharing infrastructure among a number of service providers. Consequently, deployment and managements cost-efficiencies are realized.

5.3.4 Customer Requirement

Businesses require the benefits of management ease by the most cost effective means. This can be achieved with the objective of supporting logical networks within a single set of physical WLAN equipment. There are a number of ways of realizing this objective some being virtual APs, VLAN tunnels and other tunnels.

This objective also allows for separation between providers of infrastructure from services. Logical networks allows for the separation of physical deployment and maintenance from actual management of WLANs. This helps lower costs and responsibilities for service providers.

5.3.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

5.4 Extensibility Objective

Wireless technology is developing at rapid pace in a number of industry and scientific groups. With such pace, it is important to design CAPWAP in a way as to allow future extensibility. In particular, the IEEE is in the process of specifying standards for broadband wireless access, namely IEEE 802.16. There also other activities within the IEEE that needs to be considered in the CAPWAP context.

5.4.1 Objective Details

This objective has a number of aspects that are described below;

i. Enable support for future wireless technologies

This aspect of the objective essentially purposes that the CAPWAP protocol does not rely on specifics of IEEE 802.11 technology for its operations. This will simplify extensibility to support IEEE 802.16.

ii. Enable support for new IEEE extensions

The IEEE is currently reviewing IEEE 802.11 functionality. It is expected that the review will result in new functional blocks, interfaces or information flows. The CAPWAP protocol must be able to handle these revisions with minimal changes.

iii. User(Client) Access Requirement

There should not be any impact on the end-user of CAPWAP WLAN in terms of both hardware and software aspects. End-users should not be required to be aware of the existence of CAPWAP protocol.

5.4.2 Motivation and Protocol Benefits

[TBD]

5.4.3 Relation to Problem Statement

[TBD]

5.4.4 Customer Requirements

Service providers are not enthusiastic about deploying technologies with limited potential for extension. They require WLAN infrastructure to be able to meet current and future market requirements. So the objective for extensibility is critical to service providers and other customers of WLAN equipment.

5.4.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

6. Operations Objective

CAPWAP aims to provide an interoperable solution to the control and provisioning of large scale WLAN deployments. In this context, the operational objectives address functional aspects of the protocol. These functions cover system monitoring, resource management and QoS.

6.1 WLAN Monitoring Objective

The scale of WLANs in the CAPWAP context results in numerous information sources. For example, the configuration of each WTP can be considered as an information source. Additionally, the switching segment and wireless medium segment can also be considered as information sources. So for effective performance, the CAPWAP protocol needs to regularly monitor the various information sources.

6.1.1 Objective Details

Large WLANs need a variety of information sources to be monitored. So this objective includes a number of aspects.

i. Configuration consistency

CAPWAP based WLANs include a large number of WTPs, each of which need to be configured and managed. The protocol should therefore allow WTPs to regularly send information on the state of their configuration to their WLAN controller. Furthermore, it should also be capable of consistently distributing firmware to all the WTPs.

ii. System-wide resource state

The centralized WLAN architecture is made up of a switching segment and wireless medium segment. In the switching segment, network congestion and WTP status, including firmware information, have to be monitored. In the wireless medium segment, the dynamic nature of the medium itself has to be monitored. Overall, there are also various statistics that are required for operation.

The CAPWAP protocol should therefore be capable of monitoring various information sources. Moreover, given relationships among information sources, CAPWAP should combine information from such sources. For example, statistics information may be merged with status signals. So this aspect of the objective proposes collective information arising from different information sources. Within this aspect of the monitoring objective, the protocol may also allow WTPs to send regular send feedback using CAPWAP.

6.1.2 Motivation and Protocol Benefits

The effectiveness of a protocol is based on the relevance of information on which it operates. The objective for WLAN monitoring can provide this information to the CAPWAP protocol. So there will tangible benefits with this objective.

6.1.3 Relation to Problem Statement

This objective addresses the problems of management complexity. This challenge is better solved with the appropriate information resulting from this WLAN monitoring. With collective information from various information sources, realizing this objective will help control and manage complexity.

The objective also helps address the challenge of maintaining consistent configurations among WTPs.

6.1.4 Customer Requirement

WLAN equipment customers require effective management solutions for their networks. This objective will ensure such a solution by providing collective information from a variety of information sources.

6.1.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

6.2 Resource Control Objective

Integral to the success of any wireless network system is the performance and quality it can offer its subscribers. Since CAPWAP based WLANs combine a switching segment and a wireless medium segment, performance and quality need to be coordinated across both of these segments. So QoS performance must be enforced system-wide.

6.2.1 Objective Details

This objective is for QoS over the entire WLAN system which includes the switching segment and the wireless medium segment. Given the fundamental differences between the two, it is likely that there are alternate QoS mechanisms between WTPs and wireless service subscribers and between WTPs and WLAN controllers. For instance, the former will be based on IEEE 802.11e while the latter will be an alternative. So resources need to be adjusted in a coordinated fashion over both segments. The CAPWAP protocol should ensure that

these adjustments are appropriately exchanged between WLAN controllers and WTPs.

6.2.2 Motivation and Protocol Benefits

A protocol that addresses QoS aspects of WLAN systems will deliver high performance thereby being beneficial for subscribers and resource utilization. Since CAPWAP deals with WTPs directly and with the wireless medium indirectly, both of these must be considered for performance.

For the wireless medium segment, QoS aspects in the protocol enable high quality communications within the domain of a WLAN controller. Since each domain generally covers an enterprise or a group of service providers, such protocol performance has wide-ranging effects.

Within the switching segment of CAPWAP, a QoS-enabled protocol minimizes the adverse effects of dynamic traffic characteristics so as to ensure system-wide performance.

6.2.3 Relation to Problem Statement

QoS control is critical to large WLANs and relates to a number of aspects. In particular, this objective can help address the problem of managing dynamic conditions of the wireless medium.

Furthermore, traffic characteristics in large scale WLANs are constantly varying. So network utilization becomes inefficient and user experience is unpredictable.

The interaction and coordination between the two aspects of system-wide QoS is therefore critical for performance.

6.2.4 Customer Requirements

VoIP is a major application over WLANs. The basic requirement for such applications is QoS. Furthermore, end-users demand quality means of communications, so service providers in turn emphasize on the QoS capabilities of WLAN systems. Adopting this objective will ensure all demands are met.

6.2.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

6.3 Support for Traffic Separation

The centralized WLAN architecture simplifies complexity associated with large scale deployments. This is achieved by consolidating some functionality at a central WLAN controller and distributing the remaining across WTPs. As a result, WTPs and WLAN controller exchange control and data among them. This objective suggests separating control and data aspects of the exchanges for further simplicity.

6.3.1 Objective Details

It is the aim of CAPWAP to simplify the control and management of large scale WLANs. One way of achieving this is to separate control and data aspects within the protocol. This will allow solutions for control and data exchanges to be independently optimized.

6.3.2 Motivation and Protocol Benefits

The aim of separating data and control aspects of the protocol is to simplify the protocol. It also allows for flexibility since each part can be separately addressed in the most appropriate manner.

Furthermore, such separation can also allow separation of data and control paths. This will enable remotely located WTPs to handle data in alternative ways instead of forwarding them across a wide network to the WLAN controller.

6.3.3 Relation to Problem Statement

Broadly, this objective relates to the challenge of managing complexity in large scale WLANs.

6.3.4 Customer Requirements

This objective offers simplicity and flexibility in operation. These are important issues for service providers and other enterprises deploying large scale WLANs.

6.3.5 Classification (Mandatory, Desirable, Rejected)

[TBD] [This section to contain reasons for the particular classification of the objective.]

6.4 STA Admission Control Objective

STA Admission control deals with client authentication, handoff between WTPs, load balance, QoS etc. Access control in the CAPWAP

context must be based on a variety of information. This is because CAPWAP combines both switching and wireless medium segments.

6.4.1 Objective Details

This objective focuses on access control based on collective information from the switching and wireless medium segments. As such, access to the WLAN is based on both the radio resources, i.e. wireless medium segment and network resources, i.e. switching segment.

6.4.2 Motivation and Protocol Benefits

Due to the scale of deployments in which CAPWAP will be employed, comprehensive access control is crucial. The effectiveness of access control in turn is affected by the information on which such control is based. As a result, this objective has critical relevance to a CAPWAP protocol.

6.4.3 Relation to Problem Statement

This objective addresses the issue of access control in large WLANs. Broadly, it relates the problem of managing the complexity scale of such networks. With collective information of both switching and wireless medium segments, realizing this objective will help control and manage complexity.

6.4.4 Customer Requirements

[TBD]

6.4.5 Classification (Mandatory, Desirable, Rejected)

[TBD]

6.5 Centralized WTP Management

Large scale WLAN deployments necessitate in centralized control. The CAPWAP protocol interfaces the central control to the numerous WTPs. One aspect of centralized control includes firmware distribution. This objective relates to configuration aspects of the WLAN.

7. Security Objectives

Security is a major issue for any communications network and is especially important for large scale WLANs. In this context, security must encompass both the protocol between WLAN controller and WTPs and also the WLAN system as a whole. So the following objectives deal with securing exchanges between WLAN elements and devising contingencies in case of physical security breaches.

7.1 CAPWAP Protocol Security

This objective addresses the security of the protocol.

7.1.1 Objective Details

[Note: This objective generally deals with the security between WTP and WLAN controller. It deals with threats that arise from within the network infrastructure.]

The CAPWAP protocol between WLAN controller and WTPs must be secured such that information exchange between them is not threatened. As such, it must provide confidentiality, integrity and authenticity for those exchanges.

Furthermore, CAPWAP protocol security must ensure that rogue WTPs do not breach legitimate WLAN systems. The CAPWAP protocol should therefore include authentication mechanisms for WTPs. For example, WTPs may be required to regularly renew their authentication states.

As a result of realizing this objective it should not be possible for individual WTP breaches to affect the security of the WLAN as a whole. So WTP mis-use will be protected against.

7.2 System-wide Security

[Note: This objective is to prevent against security threats from outside the CAPWAP framework. Specifically, it addresses threats posed by rogue wireless users. For example, recent discussions of PMK sharing in the CAPWAP context illustrates a situation while may be taken advantage of by a rogue wireless user. This objective differs from that of the previous section in that it deals with external threats that may affect the WLAN system.

The emphasis here is that there should be no ambiguities arising from the CAPWAP framework that causes threats from external entities.]

8. Objectives for Further Discussion

[Note: The following are some of objectives for further discussion in the WG.]

8.1 Centralized WTP Management

The CAPWAP protocol should provide an engine-mechanism to spring WTP auto-configuration and/or software version updates and should support integration with existing network management system. WLAN controller as a management agent is optional.

If entities other than WLAN controllers manage some aspects of WTPs, such as software downloads, the CAPWAP protocol may be used for WTPs to notify WLAN controllers of any changes made by the other entities.

One example of transport mechanism for the CAPWAP protocol is TCP/IP. This will bring more flexibility to the way in which WLAN systems are deployed.

8.2 Security borderline Control

[Note: This objective addresses the issue of a large WLAN infrastructure featuring the co-existence of different security policies for different user groups. It deals with traffic flow isolation on borderline of any two user groups or two users.]

8.3 Trust model Definition

[Note: When 802.1x authenticator role in 802.11i is relocated from WTP to WLAN controller, the following needs to be clarified for CAPWAP protocol development; whether there are any potential changes in the trust relationship between WTP and infrastructure. If there are changes, the new trust model needs to be defined.]

8.4 IEEE 802.11i Considerations

In the centralized WLAN architecture, authentication based on IEEE 802.11i presents options based on the location of the authenticator. Particularly, if the authenticator is located within the WLAN controller, means for key distribution need to be considered, whereas if the authenticator is within a WTP, communications between the AAA server and the WTP need to be considered. The CAPWAP protocol should therefore be able to address these options.

9. Summary and Conclusion

The objectives presented in this document address architectural, operational and security aspects for CAPWAP. They present a framework which will be used to develop and evaluate candidate protocols for managing large scale WLAN deployments.

10. Security Considerations

[Note: This section will detail the security implications of the various objectives. One way to look at it would be to analyze the security considerations of the Architecture Taxonomy and borrow/infer from it.]

The objective dealing with alternative interfaces covers the interoperability of WTPs from both local MAC and split MAC designs. As such, a WLAN controller must be capable of securing both of these design types. This may include handling different degrees of security or authentication processing for the two types of WTPs.

In shared deployments with a number of logical networks, it is crucial to ensure mutual separation of traffic among them. Access control should therefore be distinct for each of the logical networks. Furthermore, subscribers to different service providers need to be managed based on their respective requirements, subscriptions, etc. Cross exchanges need to be secured against.

It should be ensured that any stray exchanges be prevented with the automation of discovery and initialization processes.

The objective for WLAN monitoring relates to security also. Wireless systems need to be constantly monitored for potential threats in the form of rogue WTPs or terminals. For example, profiles for DoS and replay attacks need to be monitored.

In addition to securing protocol exchanges between devices in large scale WLANs, the CAPWAP protocol should also incorporate contingencies for physical security breaches. For instance, it should be ensured that the network as a whole is not compromised if a single AP is stolen or otherwise compromised. The protocol should therefore contain measures to detect and contain physical security threats.

11. Contributors

This document is the result of a merger of two individual Internet-Draft submissions. The authors of both drafts have contributed to shape this document. The authors are;

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

Satoshi Iino
Panasonic Mobile Communications
600, Saedo-cho
Tsuzuki-ku
Yokohama 224 8539
Japan
Phone: +81 45 938 3789
EMail: iino.satoshi@jp.panasonic.com

Mikihito Sugiura
Panasonic Mobile Communications
600, Saedo-cho
Tsuzuki-ku
Yokohama 224 8539
Japan
Phone: +81 45 938 3789
EMail: sugiura.mikihito@jp.panasonic.com

Dong Wang
ZTE
No.68 Zijinghua Rd, Yuhuatai District
Tsuzuki-ku
Nanjing, Jiangsu Prov. 210 012
P. R. China
Phone: +86 25 5287 1713
EMail: wang.dong@mail.zte.com.cn

12. Acknowledgements

The authors would like to thank the Working Group Chairs, Dorothy Gellert and Mahalingam Mani, for their support and patience with this document. We would also like to thank participants of the Working Group who have helped shape the objectives. In particular, the authors thank Pat Calhoun and Inderpreet Singh for their invaluable inputs.

13 References

[Functionality Classifications]
Cheng, H. et al, "Functionality Classifications for Control and Provisioning of Wireless Access Points", draft-cheng-capwap-classifications-01, (work in progress), July 2004.

[I-D.ietf-capwap-arch]
Yang, L., Zerfos, P. and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points(CAPWAP)", draft-ietf-capwap-arch-06 (work in progress), November 2004.

[I-D.ietf-capwap-problem-statement]
Calhoun, P., "CAPWAP Problem Statement", draft-ietf-capwap-problem-statement-02 (work in progress), September 2004.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Saravanan Govindan
Panasonic Singapore Laboratories
Block 1022, Tai Seng Industrial Estate
#06-3530, Tai Seng Avenue
Singapore 534 415
Singapore

Phone: +65 6550 5441
EMail: sgovindan@psl.com.sg

Zhonghui Yao
Huawei Longgang Production Base
Shenzhen 518 129
P. R. China

Phone: +86 755 2878 0808
EMail: yaoth@huawei.com

Wenhui Zhou
China Mobile
53A, Xibianmen Ave, Xuanwu District
Beijing 100 053
P. R. China

Phone: +86 10 6600 6688 ext.3061
EMail: zhouwenhui@chinamobile.com

L. Lily Yang
Intel Corp.
JF3-206, 2111 NE 25th Ave.
Hilsboro, OR 97124
USA

Phone: +1 503 264 8813
EMail: lily.l.yang@intel.com

Hong Cheng
Panasonic Singapore Laboratories
Block 1022, Tai Seng Industrial Estate
#06-3530, Tai Seng Avenue
Singapore 534 415
Singapore

Phone: +65 6550 5447
EMail: hcheng@psl.com.sg

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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