Network Working Group
Request for Comments: 4564
Category: Informational

S. Govindan, Ed.
H. Cheng
Panasonic
ZH. Yao
Huawei
WH. Zhou
China Mobile
L. Yang
Intel

July 2006

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

Status of This Memo

Copyright Notice

Abstract

This document presents objectives for an interoperable protocol for the Control and Provisioning of Wireless Access Points (CAPWAP). The document aims to establish a set of focused requirements for the development and evaluation of a CAPWAP protocol. The objectives address architecture, operation, security, and network operator requirements that are necessary to enable interoperability among Wireless Local Area Network (WLAN) devices of alternative designs.

Table of Contents

1. Introduction

The growth in large-scale Wireless Local Area Network (WLAN) deployments has brought into focus a number of technical challenges. Among them is the complexity of managing large numbers of Wireless Termination Points (WTPs), which is further exacerbated by variations in their design. Another challenge is the maintenance of consistent configurations among the numerous WTPs of a system. The dynamic nature of the wireless medium is also a concern together with WLAN security. The challenges affecting large-scale WLAN deployments have been highlighted in [RFC3990].

Many vendors have addressed these challenges by developing new architectures and solutions. A survey of the various developments was conducted to better understand the context of these challenges. This survey is a first step towards designing interoperability among the solutions. The Architecture Taxonomy [RFC4118] is a result of this survey in which major WLAN architecture families are classified. Broadly, these are the autonomous, centralized WLAN, and distributed mesh architectures.

The Architecture Taxonomy identified the centralized WLAN architecture as one in which portions of the wireless medium access control (MAC) operations are centralized in a WLAN controller. This centralized WLAN architecture is further classified into remote-MAC, split-MAC, and local-MAC designs. Each differs in the degree of separation of wireless MAC layer capabilities between WTPs and WLAN controller.

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

2. Terminology

This document uses terminology defined in [RFC4118], [802.11], [802.11i], and [802.11e]. Additionally, the following terms are defined.

Centralized WLAN: A WLAN based on the centralized WLAN Architecture [RFC4118].

Switching Segment: Those aspects of a centralized WLAN that primarily deal with switching or routing of 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 wireless interface between WTPs and wireless terminals. The Wireless Medium Segment is specific to layer 2 wireless technology, such as IEEE 802.11.

CAPWAP Framework: A term that covers the local-MAC and split-MAC designs of the Centralized WLAN Architecture. Standardization efforts are focused 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.

Logical Group: A logical separation of a physical WTP is termed logical group. So a single physical WTP will operate a number of logical groups. Virtual access points (APs) are examples of logical groups. Here, each Basic Service Set Identifier (BSSID) and constituent wireless terminals' radios are denoted as distinct logical groups of a physical WTP. Logical groups are maintained without conflicting with the CAPWAP objectives, particularly the 'Wireless Terminal Transparency' objective.

3. 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].

4. Objectives Overview

The objectives for CAPWAP have been broadly classified to address architecture, operation, and security requirements of managing large-scale WLAN deployments.

Architecture objectives deal with system-level aspects of the CAPWAP protocol. They address issues of protocol extensibility, diversity in 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 WLAN monitoring, resource management, Quality of Service (QoS), and access control.

Security objectives address potential threats to WLANs and their containment. In the CAPWAP context, security requirements cover the protocol between the WLAN controller and WTPs and also the WLAN system as a whole.

Additionally, a general classification is used for objectives relating to the overall impact of the CAPWAP protocol specifications.

5. Objectives

The objectives described in this document have been prioritized based on their immediate significance in the development and evaluation of a control and provisioning protocol for large-scale WLAN deployments. The priorities are:

i. Mandatory and Accepted Objectives
ii. Desirable Objectives
iii. Non-Objectives

The priorities have been assigned to individual objectives in accordance with working group discussions.

Furthermore, a distinct category of objectives is provided based on requirements gathered from network service operators. These are specific needs that arise from operators' experiences in deploying and managing large-scale WLANs.

a. Operator Requirements

5.1. Mandatory and Accepted Objectives

Objectives prioritized as mandatory and accepted have been deemed crucial for the control and provisioning of WTPs. They directly address the challenges of large-scale WLAN deployments and MUST be realized by a CAPWAP protocol.

5.1.1. Logical Groups

Classification: Architecture

Description:

Large WLAN deployments are complex and expensive. Furthermore, enterprises deploying such networks are under pressure to improve the efficiency of their expenditures.

Shared WLAN deployments, where a single physical WLAN infrastructure supports a number of logical networks, are increasingly used to address these two issues of large-scale WLANs. These are popular as they allow deployment and management costs to be spread across businesses.

In traditional WLANs, each physical WTP represents one complete subset of a larger WLAN system. Shared WLANs differ in that each physical WTP represents a number of logical subsets of possibly a number of larger WLAN systems. Each logical division of a physical WTP is referred to as a logical group (see definition in Section 2). So WLANs are managed in terms of logical groups instead of physical WTPs. Logical groups are based on BSSIDs and other types of virtual APs.

Protocol Requirement:

The CAPWAP protocol MUST be capable of controlling and managing physical WTPs in terms of logical groups including BSSID-based groups.

For all operating modes, including those in which the WTP performs local bridging and those in which the Access Controller (AC) performs centralized bridging, the protocol MUST provide provisions for configuring logical groups at the WTP.

Motivation and Protocol Benefits:

Commercial realities necessitate that WLANs be manageable in terms of their logical groups. This allows separation of logical services and underlying infrastructure management. A protocol that realizes this need ensures simpler and cost-effective WLANs, which directly address the requirements of network service operators.

Relation to Problem Statement:

This objective addresses the problem of management complexity in terms of costs. Cost complexity is reduced by sharing WLAN deployments. Consequently, deployment and management cost-efficiencies are realized.

5.1.2. Support for Traffic Separation

Classification: Operations

Description:

The centralized WLAN architecture simplifies complexity associated with large-scale deployments by consolidating portions of wireless MAC functionality at a central WLAN controller and distributing the remaining across WTPs. As a result, WTPs and WLAN controller exchange control and data information between them. This objective

states that control and data aspects of the exchanges be mutually separated for further simplicity. This will allow solutions for each type of exchange to be independently optimized.

Furthermore, in the context of shared WLAN deployments, the mutual separation of control and data also addresses security concerns. In particular, given the likelihood of different logical groups, such as those established by different virtual APs, being managed by different administrators, separation of control and data is a first step towards individually containing and securing the logical groups.

It is also important to ensure that traffic from each logical group is mutually separated to maintain the integrity and independence of the logical groups.

Protocol Requirement:

The CAPWAP protocol MUST define transport control messages such that the transport of control messages is separate from the transport of data messages.

Motivation and Protocol Benefits:

The aim of separating data and control aspects of the protocol is to simplify the protocol. It also allows for the flexibility of addressing each type of traffic in the most appropriate manner.

Furthermore, this requirement will help remotely located WTPs to handle data traffic in alternative ways without the need for forwarding them across a wide network to the WLAN controller.

Separation of WTP control and data also aids in the secure realization of shared WLAN deployments.

Relation to Problem Statement:

Broadly, this objective relates to the challenge of managing complexity in large-scale WLANs. The requirement for traffic separation simplifies control as this is separated from the task of data transport.

5.1.3. Wireless Terminal Transparency

Classification: Operations

Description:

The CAPWAP protocol is applicable between a centralized WLAN controller and a number of WTPs; i.e., it affects only the switching segment of the centralized WLAN architecture. Its operations should therefore be independent of the wireless terminal. Wireless terminals should not be required to be aware of the existence of the CAPWAP protocol.

Protocol Requirement:

Wireless terminals MUST NOT be required to recognize or be aware of the CAPWAP protocol.

Motivation and Protocol Benefits:

IEEE 802.11-based wireless terminals are mature and widely available. It would be beneficial for CAPWAP not to impose new requirements on these wireless terminals. In effect, this requirement ensures that the setup cost of the protocol is reduced as the numerous existing wireless terminals need not be altered.

Relation to Problem Statement:

The Problem Statement highlights the challenges faced by large WLANs consisting of many WTPs. It does not refer to the operations of wireless terminals and this objective emphasizes the independence.

5.1.4. Configuration Consistency

Classification: Operations

Description:

WLANs in the CAPWAP framework contain numerous WTPs, each of them needing to be configured and managed in a consistent manner. The main concern in ensuring consistency is availability of appropriate information corresponding to WTP configuration states. So configuration consistency can be achieved by providing the centralized WLAN controller with regular updates on the state of WTP operations. The centralized WLAN controller can in turn apply information from the regular updates to ensure consistently among the WTPs.

Protocol Requirement:

The CAPWAP protocol MUST include support for regular exchanges of state information between WTPs and the WLAN controller. Examples of state information include WTP processing load and memory utilization.

Motivation and Protocol Benefits:

A protocol that provides access to regular state information can in turn be used to enhance WLAN configuration and performance. The CAPWAP protocol will be better equipped to address configuration-related problems with the regularly available state information. So with greater state information, control and management operations can be improved.

Relation to Problem Statement:

One of the major challenges described in the Problem Statement is that of maintaining consistent configuration across the numerous WTPs of a WLAN. This objective addresses the fundamental issue behind this -- availability of timely state information.

5.1.5. Firmware Trigger

Classification: Operations

Description:

One specific aspect of configuration consistency is the firmware used by various WTPs. The scale of large WLANs introduces possibilities for variations in the firmware used among WTPs. This objective highlights the need for the CAPWAP protocol to trigger the delivery of appropriate versions of firmware to WTPs. The actual delivery of firmware need not be inclusive to the protocol.

Protocol Requirement:

The CAPWAP protocol MUST support a trigger for delivery of firmware updates.

Motivation and Protocol Benefits:

The CAPWAP protocol interfaces many WTPs to a centralized WLAN controller. Firmware distribution allows these interfaces to be compatible. This in turn results in consistent configuration and simplified management. So the protocol benefits by including triggers for the distribution of firmware updates.

Relation to Problem Statement:

Inconsistencies in the configuration of WTPs have been identified as a major challenge for large-scale WTPs. This objective helps overcome the challenge by providing a way for the CAPWAP protocol to initiate delivery of firmware updates that are compatible among all WTPs.

5.1.6. Monitoring and Exchange of System-wide Resource State

Classification: Operations

Description:

The centralized WLAN architecture is made up of a switching segment and wireless medium segment. In the switching segment, network congestion, WTP status, and 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 need to be considered for efficient WLAN operation.

The CAPWAP protocol should be capable of monitoring the various information sources and deliver the resulting information to the relevant WLAN devices -- either WTPs or the WLAN controller. Moreover, given the relationship among information sources, the CAPWAP protocol should combine state information from them. For example, statistics information and status signals from WTPs may be merged before being exchanged.

Examples of statistics information that the CAPWAP protocol should monitor and exchange include congestion state, interference levels, loss rates, and various delay factors.

Protocol Requirement:

The CAPWAP protocol MUST allow for the exchange of statistics, congestion, and other WLAN state information.

Motivation and Protocol Benefits:

The effectiveness of a protocol is based on the relevance of information on which it operates. This requirement for resource monitoring and exchange can provide the appropriate information to the CAPWAP protocol.

Relation to Problem Statement:

The Problem Statement highlights the challenge of dealing with large numbers of WTPs and the dynamic nature of the wireless medium. Information on the state of WTPs and the medium is important to deal with them effectively. So this objective relates to the problem of managing consistency in large WLANs.

5.1.7. Resource Control Objective

Classification: Operations

Description:

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.

This objective highlights 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, whereas 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.

In addition to IEEE 802.11e, there are a number of other IEEE 802.11 task groups that may affect network resources. These include IEEE 802.11 TGk, TGu, and TGv, which are currently in progress. CAPWAP should therefore not be restricted to IEEE 802.11e-based mapping.

Protocol Requirement:

The CAPWAP protocol MUST map the IEEE 802.11e QoS priorities to equivalent QoS priorities across the switching and wireless medium segments.

Motivation and Protocol Benefits:

A protocol that addresses QoS aspects of WLAN systems will deliver high performance thereby being beneficial for subscribers and for resource utilization efficiency. 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.

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 are therefore critical for performance.

5.1.8. CAPWAP Protocol Security

Classification: Security

Description:

This objective addresses the security of the CAPWAP protocol.

The CAPWAP protocol MUST first provide for the participating entities -- the WLAN controller and WTPs -- to be explicitly mutually authenticated. This is to ensure that rogue elements do not gain access to the WLAN system. Rogue WTPs should not be allowed to breach legitimate WLANs, and at the same time rogue WLAN controllers should not be allowed to gain control of legitimate WTPs. For example, WTPs may need to regularly renew their authentication state with the WLAN controller and similarly for WLAN controllers.

If authentication is performed via an authenticated key exchange, future knowledge of derived keys is not sufficient for authentication.

Any session keys used between the WLAN controller and WTPs MUST be mutually derived using entropy contributed by both parties. This ensures that no one party has control over the resulting session keys.

Once WTPs and the WLAN controller have been mutually authenticated, information exchanges between them must be secured against various security threats. So the CAPWAP protocol MUST provide integrity protection and replay protection. The protocol SHOULD provide confidentiality through encryption. This should cover illegitimate modifications to protocol exchanges, eavesdropping, and Denial of Service (DoS) attacks, among other potential compromises. So the protocol must provide confidentiality, integrity, and authenticity for those exchanges.

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 misuse will be protected against.

Additionally, the key establishment protocol for authentication and securing CAPWAP exchanges must be designed to minimize the possibility of future compromises after the keys are established.

CAPWAP MUST NOT prevent the use of asymmetric authentication. The security considerations of such asymmetric authentication are described in the Security Considerations section.

If the CAPWAP protocol meets the criteria to require automated key management per BCP 107 [RFC4107], then mutual authentication MUST be accomplished via an authenticated key exchange.

Protocol Requirement:

The CAPWAP protocol MUST support mutual authentication of WTPs and the centralized controller. It also MUST ensure that information exchanges are integrity protected and SHOULD ensure confidentiality through encryption.

Motivation and Protocol Benefits:

WLANs are increasingly deployed in critical aspects of enterprise and consumer networks. In these contexts, protocol security is crucial to ensure the privacy and integrity expected from network administrators and end-users. So securing the CAPWAP protocol has direct benefits in addressing these concerns.

In many cases, the network path between a WTP and WLAN controller contains untrusted links. Such links could be leveraged by rogue WTPs to gain access to the WLAN system. They could also be used by rogue WLAN controllers to gain control of legitimate WTPs and their associated terminals to either redirect or compromise terminal traffic. These security concerns can be mitigated with this objective.

Relation to Problem Statement:

Security problems in large-scale WLANs are detailed in the Problem Statement. These include complications arising from rogue WTPs and compromised interfaces between WTPs and the WLAN controller. The requirement for protocol security addresses these problems and highlights the importance of protecting against them.

5.1.9. System-wide Security

Classification: Security

Description:

The emphasis of this objective is on the security threats external to the centralized CAPWAP segment of a WLAN system. The focus is therefore on rogue wireless clients and other illegitimate wireless interferences. There are a number of specific external threats that need to be addressed within the CAPWAP framework.

i. PMK Sharing

One aspect of this objective relates to recent discussions on Pairwise Master Key (PMK) sharing in the CAPWAP framework. This objective highlights the need to prevent exploitation of this ambiguity by rogue wireless clients. It is to ensure that any ambiguities arising from the CAPWAP framework are not cause for security breaches.

Protocol Requirement:

The design of the CAPWAP protocol MUST NOT allow for any compromises to the WLAN system by external entities.

Motivation and Protocol Benefits:

The external threats to the centralized WLAN architecture become increasingly crucial given the low cost of wireless clients. Since it is relatively inexpensive for rogue individuals to mount attacks, it is important that WLAN systems are protected against them. Adequate mechanisms to thwart such external threats will be of tremendous benefit to the WLAN systems controlled and managed with the CAPWAP protocol.

Relation to Problem Statement:

This objective is based on the security needs highlighted in the Problem Statement. Specifically, the Problem Statement discusses the effects of the shared wireless medium. This represents the external aspects of the CAPWAP framework from which certain threats can arise. The system-wide security objective addresses such threats in relation to the Problem Statement.

5.1.10. IEEE 802.11i Considerations

Classification: Operations

Description:

The CAPWAP protocol must support authentication in the centralized WLAN architecture in which the authenticator and encryption points can be located on distinct entities, i.e., WLAN controller or WTP. The Architecture Taxonomy illustrates a number of variants, in both local-MAC and split-MAC designs, in which the authenticator is located at the WLAN controller and the encryption points are at the WTPs. The CAPWAP protocol must be applicable to these variants and allow authentication mechanisms and their constituent processes to be operable in these cases.

An important issue to consider in this case is the exchange of key information when authenticator and encryption points are located on distinct entities. For example, consider the case where IEEE 802.11i is used in a WLAN in which the WLAN controller realizes the authenticator, some WTPs realize encryption (possibly local-MAC WTPs), and other WTPs rely on the WLAN controller for encryption (possibly split-MAC WTPs).

Here, CAPWAP will first need to identify the location of the authenticator and encryption points between each WLAN controller-WTP pair. This will likely be part of the initial WTP configuration. Subsequently, the WTPs that realize encryption will need CAPWAP to exchange key information with the authenticator at the WLAN controller. For the WTPs that do not realize encryption, CAPWAP needs to adapt its control to bypass the key exchange phase.

Clearly, the centralized WLAN architecture presents a different platform for authentication mechanisms compared to legacy WLANs in which a WTP realized both authenticator and encryption roles. So this objective highlights the need for CAPWAP to support authentication and key management in the centralized WLAN architecture.

Protocol Requirement:

The CAPWAP protocol MUST determine the exact structure of the centralized WLAN architecture in which authentication needs to be supported, i.e., the location of major authentication components. This may be achieved during WTP initialization where major capabilities are distinguished.

The protocol MUST allow for the exchange of key information when authenticator and encryption roles are located in distinct entities.

Motivation and Protocol Benefits:

The immediate focus of CAPWAP is on supporting IEEE 802.11-based WLANs. As such, it is necessary for the protocol to recognize the major distinction in WLAN design with respect to IEEE 802.11i authenticator and encryption points. This represents a significant variation that has been highlighted in the Architecture Taxonomy. The CAPWAP protocol benefits by accommodating such a major consideration from IEEE 802.11i.

These requirements will be common for all authentication mechanisms over the centralized WLAN architecture. So they are applicable to IEEE 802.11i, Universal Access Method (UAM), and other mechanisms.

Relation to Problem Statement:

The Problem Statement highlights the availability of different WTP designs and the need to ensure interoperability among them. In this regard, operational changes occurring due to the separation of the IEEE 802.11i authenticator and encryption points need to be accommodated within the CAPWAP protocol.

5.1.11. Interoperability Objective

Classification: Architecture

Description:

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.

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. Capability negotiations between WLAN controller and WTPs

WTP designs differ in the degree of IEEE 802.11 MAC functionalities that each type of WTP realizes. The major distinctions, split-MAC and local-MAC, differ in the processing of IEEE 802.11 MAC frames. In this regard, the CAPWAP protocol should include functionality that allows for negotiations of significant capabilities between WTPs and the WLAN controller.

As a first step, such negotiations could cover the type of WTP, split-MAC or local-MAC, as this provides substantial information on their respective capabilities.

ii. Establishment of alternative interfaces

The capability differences among different WTPs essentially equate to alternative interfaces with a WLAN controller. So the CAPWAP protocol should be capable of adapting its operations to the major different interfaces. In a first case, this would include accommodating capability differences between local-MAC and split-MAC WTPs.

The definition of these interfaces in terms of finer granularity of functionalities will be based on AP functionality documents produced by the IEEE 802.11 AP Functionality (APF) Ad-Hoc Committee.

Protocol Requirement:

The CAPWAP protocol MUST include sufficient capabilities negotiations to distinguish between major types of WTPs.

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. The Architecture Taxonomy tabulates major common features of the two 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.

Relation to Problem Statement:

The objective for supporting both local-MAC and split-MAC WTPs is fundamental to addressing the 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 mechanisms that address the challenges of large-scale WLAN deployments.

5.1.12. Protocol Specifications

Classification: General

Description:

WLAN equipment vendors require sufficient details from protocol specifications so that implementing them will allow for compatibility with other equipment that runs the same protocol. In this light, it is important for the CAPWAP protocol specifications to be reasonably complete for realization.

Protocol Requirement:

Any WTP or WLAN controller vendor or any person MUST be able to implement the CAPWAP protocol from the specification itself and by that it is required that all such implementations do interoperate.

Motivation and Protocol Benefits:

It is beneficial for WLAN equipment vendors to refer to a single set of specifications while implementing the CAPWAP protocol. This helps to ease and quicken the development process.

Relation to Problem Statement:

This requirement is based on WG discussions that have been determined to be important for CAPWAP.

5.1.13. Vendor Independence

Classification: General

Description:

Rapid developments in WLAN technologies result in equipment vendors constantly modifying their devices. In many cases, developments are independently made for WLAN controllers and WTPs. The CAPWAP protocol should not affect the independence of device modifications.

Protocol Requirement:

A WTP vendor SHOULD be able to make modifications to hardware without any WLAN controller vendor involvement.

Motivation and Protocol Benefits:

Independence in the type of hardware for WLAN equipment ensures that new developments do not hamper protocol operation.

Relation to Problem Statement:

This requirement is based on WG discussions that have been determined to be important for CAPWAP.

5.1.14. Vendor Flexibility

Classification: General

Description:

The CAPWAP protocol must not be specified for a particular type of wireless MAC design. It should be compatible with both local-MAC and split-MAC WTPs.

Protocol Requirement:

The CAPWAP protocol MUST NOT limit WTP vendors in their choice of local-MAC or split-MAC WTPs. It MUST be compatible with both types of WTPs.

Motivation and Protocol Benefits:

This requirement is to ensure that WTP vendors have sufficient flexibility in selecting the type of wireless MAC design that they consider best for deployments.

Relation to Problem Statement:

This requirement is based on WG discussions that have been determined to be important for CAPWAP.

5.1.15. NAT Traversal

Classification: General

Description:

WLAN deployments may involve WTPs and the WLAN controller communicating across Network Address Translators (NATs). The CAPWAP protocol must be capable of operating across topologies that contain known NAT configurations. It requires appropriate discovery and identification mechanisms for NAT traversal.

Protocol Requirement:

The CAPWAP protocol MUST NOT prevent the operation of established methods of NAT traversal.

Motivation and Protocol Benefits:

The widespread adoption of WLANs raises the possibility for WLAN topologies containing NATs. It is important for the CAPWAP protocol to be applicable within such topologies. This requirement aims to make the CAPWAP protocol relevant for NAT traversal.

Relation to Problem Statement:

This requirement is based on WG discussions that have been determined to be important for CAPWAP.

5.2. Desirable Objectives

These objectives have been determined to be desirable for a CAPWAP protocol but not mandatory. Realizing these objectives may help improve control of WLANs but need not necessarily be required for all networks or scenarios.

5.2.1. Multiple Authentication Mechanisms

Classification: Architecture

Description:

Shared WLAN infrastructure raises the issue of multiple authentication mechanisms. This is because each logical group is likely to be associated with different service providers or WLAN domains. As a result, the authentication needs within them will be different. Although CAPWAP is required to support IEEE 802.11i, it is also necessary for it to support other authentication mechanisms. For example, one logical group may use IEEE 802.11i, whereas another may use web authentication. CAPWAP must be able to operate in such shared WLANs.

Protocol Requirement:

The CAPWAP protocol MUST support different authentication mechanisms in addition to IEEE 802.11i.

Motivation and Protocol Benefits:

The benefit of supporting various authentication mechanisms is that the protocol then becomes flexible for use in various deployments. The protocol will therefore not mandate the use of any particular mechanisms that may not be appropriate for a particular deployment.

Relation to Problem Statement:

This objective relates to the problem of management complexity. Shared WLAN deployments simplify management of large networks.

5.2.2. Support for Future Wireless Technologies

Classification: Architecture

Description:

The rapid pace of technology developments means that new advances need to be catered to in current analyses. Among these is the

support for new wireless technologies within the CAPWAP protocol, such as IEEE 802.16. The protocol should therefore not rely on specifics of IEEE 802.11 technology.

In all cases where the CAPWAP protocol messages contain specific layer 2 information elements, the definition of the protocol needs to provide for extensibility so that these elements can be defined for specific layer 2 wireless protocols. This may entail assigning a layer 2 wireless protocol type and version field to the message PDU. Examples of other wireless protocols that might be supported include but are not limited to 802.16e, 802.15.x, etc.

Protocol Requirement:

CAPWAP protocol messages MUST be designed to be extensible for specific layer 2 wireless technologies. It should not be limited to the transport of elements relating to IEEE 802.11.

Motivation and Protocol Benefits:

There are many benefits to an extensible protocol. It allows for application in different networks and provides greater scope. Furthermore, service providers require WLAN solutions that will be able to meet current and future market requirements.

Relation to Problem Statement:

The Problem Statement describes some of the advances taking place in other standards bodies like the IEEE. It is important for the CAPWAP protocol to reflect the advances and provide a framework in which they can be supported.

5.2.3. Support for New IEEE Requirements

Classification: Architecture

Description:

The IEEE 802.11 APF Ad-Hoc Committee has reviewed IEEE 802.11 functionality and has made more thorough definitions for the new requirements. The CAPWAP protocol must be able to incorporate these definitions with minimal change. Furthermore, a number of extensions for IEEE 802.11 are currently being standardized. The CAPWAP protocol must also be able to incorporate these new extensions with minimal change.

Protocol Requirement:

The CAPWAP protocol MUST be openly designed to support new IEEE 802.11 definitions and extensions.

Motivation and Protocol Benefits:

There are a number of advances being made within the IEEE regarding the functionality of IEEE 802.11 technology. Since this represents one of the major wireless technologies in use today, it will be beneficial for CAPWAP to incorporate the relevant new extensions.

Relation to Problem Statement:

The Problem Statement presents an overview of the task of the IEEE 802.11 working group. This group is focused on defining the functional architecture of WTPs and new extensions for it. It is necessary for the CAPWAP protocol to reflect these definitions and extensions.

5.2.4. Interconnection Objective

Classification: Architecture

Description:

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 various interconnection technologies.

As a result of realizing this objective, the protocol will be capable of operation over both IPv4 and IPv6. It will also be designed such that it can operate within tightly administered networks, such as enterprise networks, or on open, public access networks. For example, VLAN tunnels can be used across different types of networks over which CAPWAP will operate.

Protocol Requirement:

The CAPWAP protocol MUST NOT be constrained to specific underlying transport mechanisms.

Motivation and Protocol Benefits:

The main aim of the CAPWAP protocol is to achieve interoperability among various WTPs and WLAN controllers. As such, the motivation for this requirement is for the protocol to be operable independent of underlying interconnection technologies.

Relation to Problem Statement:

The Problem Statement discusses the complexity of configuring large WLANs. The selection of available interconnection technologies for large-scale deployments further intensifies this complexity. This requirement avoids part of the complexity by advocating independence of the operational aspects of the protocol from underlying transport.

5.2.5. Access Control

Classification: Operations

Description:

This objective focuses on the informational needs of WLAN access control and specifically the role of the CAPWAP protocol in transporting this information between WTPs and their WLAN controller.

The following are some specific information aspects that need to be transported by the CAPWAP protocol:

i. IEEE 802.11 association and authentication

The association of wireless clients is distinct for initial and roaming cases. As a result, access control mechanisms require specific contextual information regarding each case. Additionally, load balancing, QoS, security, and congestion information in both wireless medium segments and switching segments need to be considered.

ii. WTP Access Control

In addition to controlling access for wireless clients, it is also necessary to control admission of new WTPs. Given the threat of rogue WTPs, it is important for CAPWAP to relay appropriate authentication information between new WTPs and the WLAN controller.

Protocol Requirement:

The CAPWAP protocol MUST be capable of exchanging information required for access control of WTPs and wireless terminals.

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.

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.

5.3. Non-Objectives

The following objectives have been prioritized as non-objectives during the course of working group consultations. They have been prioritized so in the context of CAPWAP and its considerations. They may, however, be applicable in alternative contexts.

5.3.1. Support for Non-CAPWAP WTPs

Classification: Architecture

Description:

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.

Protocol Requirement:

The CAPWAP protocol SHOULD be capable of recognizing legacy WTPs and existing network management systems.

Motivation and Protocol Benefits:

It is expected that in many cases, the centralized WLAN architecture will be deployed incrementally with legacy systems. In this regard, it is necessary for the protocol to be used in scenarios with mixed WLAN devices.

Relation to Problem Statement:

The Problem Statement highlights management complexity as a major issue with large WLANs. One part of this complexity can be related to the incremental deployment of centralized WLAN devices for which this objective is applicable.

5.3.2. Technical Specifications

Classification: General

Description:

The CAPWAP protocol must not require AC and WTP vendors to share technical specifications to establish compatibility. The protocol specifications alone must be sufficient for compatibility.

Protocol Requirement:

WTP vendors SHOULD NOT have to share technical specifications for hardware and software to AC vendors in order for interoperability to be achieved.

Motivation and Protocol Benefits:

It is beneficial for WLAN equipment vendors to refer to a single set of specifications while implementing the CAPWAP protocol. This helps to ease and quicken the development process.

Relation to Problem Statement:

This requirement is based on WG discussions that have been determined to be important for CAPWAP.

This objective has been prioritized as a non-objective as it is a duplicate of the Protocol Specifications objective (Section 5.1.12).

5.4. Operator Requirements

The following objectives have been provided by network service operators. They represent the requirements from those ultimately deploying the CAPWAP protocol in their WLANs.

5.4.1. AP Fast Handoff

Classification: Operations

Description:

Network service operators consider handoffs crucial because of the mobile nature of their customers. In this regard, the CAPWAP protocol should not adversely affect AP fast-handoff procedures. The protocol may support optimizations for fast handoff procedures so as to allow better support for real-time services during handoffs.

Protocol Requirement:

CAPWAP protocol operations MUST NOT impede or obstruct the efficacy of AP fast-handoff procedures.

6. Summary and Conclusion

The objectives presented in this document address three main aspects of the CAPWAP protocol, namely:

i. Architecture
ii. Operations
iii. Security

These requirements are aimed at focusing standardization efforts on a simple, interoperable protocol for managing large-scale WLANs. The architecture requirements specify the structural features of the protocol such as those relating to WTP types (local-MAC and split-MAC) and WTP structures (logical groups). The operations requirements address the functional aspects dealing with WTP configuration and management. Finally, the security requirements cover authentication and integrity aspects of protocol exchanges.

The objectives have additionally been prioritized to reflect their immediate significance to the development and evaluation of an interoperable CAPWAP protocol. The priorities are Mandatory and Accepted, Desirable, and Non-Objectives. They reflect working group consensus on the effectiveness of the requirements in the context of protocol design.

Additionally, this document includes requirements from network service operators that have been derived based on their experience in operating large-scale WLANs.

The resulting requirements from this document will be used in conjunction with the CAPWAP Problem Statement [RFC3990] and CAPWAP Architecture Taxonomy [RFC4118] to develop and evaluate an interoperable protocol for the control and provisioning of WTPs in large-scale WLANs.

7. Security Considerations

The CAPWAP framework highlights support for both local-MAC and split-MAC WTPs. In deployments where both types of WTPs are used, it is crucial to ensure that each be secured in consideration of its capabilities. The Architecture Taxonomy illustrates how different WTPs incorporate varying levels of functionalities. Development of the CAPWAP protocol should ensure that the deployment of both local-MAC and split-MAC WTPs within a single WLAN do not present loopholes for security compromises.

In shared WLAN deployments made of a number of logical groups, traffic from each group needs to be mutually separated. So in addition to protocol-related exchanges, data traffic from wireless terminals should also be segregated with respect to the logical groups to which they belong. It should not be possible for data or control traffic from one logical group to stray to or influence another logical group.

The use of IEEE 802.11i over the centralized WLAN architecture allows for implementations in which the PMK is shared across WTPs. This raises the ambiguity between legitimate sharing and illegitimate copies. Wireless terminals may unknowingly fall prey to or exploit this ambiguity. The resolution of this issue is currently being evaluated by the IEEE 802 and IETF liaisons.

The low cost of launching attacks on WLANs makes the CAPWAP protocol a target. A first step in securing against any form of attacks is to continuously monitor the WLAN for conditions of potential threats from rogue WTPs or wireless terminals. For example, profiles for DoS and replay attacks need to be considered for the CAPWAP protocol to effectively monitor security conditions.

The open environment of many WLAN deployments makes physical security breaches highly probable. Compromises resulting from theft and physical damage must be considered during protocol development. For instance, it should not be possible for a single compromised WTP to affect the WLAN as a whole.

Considering asymmetric, non-mutual authentication between WTPs and the WLAN controller, there is a risk of a rogue participant exploiting such an arrangement. It is preferable to avoid non-mutual authentication. In some cases, the legitimacy of the protocol exchange participants may be verified externally, for example, by means of physical containment within a close environment. Asymmetric authentication may be appropriate here without risk of security compromises.

8. 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 James Kempf, Pat Calhoun, Inderpreet Singh, Dan Harkins, T. Sridhar, Charles Clancy, and Emek Sadot for their invaluable inputs. We also extend our gratitude to the IEEE 802.11 Ad-Hoc Committee for its evaluation of the document. The authors also acknowledge the contributions from Meimei Dang, Satoshi Iino, Mikihito Sugiura, and Dong Wang.

9. Normative References

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

[RFC3990] O'Hara, B., Calhoun, P., and J. Kempf, "Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement", RFC 3990, February 2005.

[RFC4118] Yang, L., Zerfos, P., and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4118, June 2005.

10. Informative References

[802.11] IEEE Standard 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", June 2003.

[802.11i] IEEE Standard 802.11i, "Medium Access Control (MAC) Security Enhancements", July 2004.

[802.11e] IEEE Standard 802.11e, "Medium Access Control (MAC) Quality of Service Enhancements", November 2005.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

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: saravanan.govindan@sg.panasonic.com

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: hong.cheng@sg.panasonic.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).