       Configuration and Provisioning for Wireless Access Points (CAPWAP)
                            Problem Statement

Status of This Memo

Copyright Notice

Abstract

   This document describes the Configuration and Provisioning for
   Wireless Access Points (CAPWAP) problem statement.

1. Introduction

   With the approval of the 802.11 standard by the IEEE in 1997,
   wireless LANs (WLANs) began a slow entry into enterprise networks.
   The limited data rates of the original 802.11 standard, only 1 and 2
   Mbps, limited the widespread adoption of the technology. 802.11
   found wide deployment in vertical applications, such as inventory
   management, point of sale, and transportation management. Pioneering
   enterprises began to deploy 802.11, mostly for experimentation.

   In 1999, the IEEE approved the 802.11a and 802.11b amendments to the
   base standard, increasing the available data rate to 54 and 11 Mbps,
   respectively, and expanding to a new radio band. This removed one of
   the significant factors holding back adoption of 802.11 in large
   enterprise networks. These large deployments were bound by the
   definition and functionality of an 802.11 Access Point (AP), as
   described in the 802.11 standard. The techniques required extensive
   use of layer 2 bridging and widespread VLANs to ensure the proper
   operation of higher layer protocols. Deployments of 802.11 WLANs as
   large as several thousand APs have been described.

Large deployments of 802.11 WLANs have introduced several problems
that require solutions. The limitations on the scalability of
bridging should come as no surprise to the networking community, as
similar limitations arose in the early 1980s for wired network
bridging during the expansion and interconnection of wired local area
networks. This document will describe the problems introduced by the
large-scale deployment of 802.11 WLANs in enterprise networks.

2. Problem Statement

Large WLAN deployments introduce several problems. First, each AP is
an IP-addressable device requiring management, monitoring, and
control. Deployment of a large WLAN will typically double the number
of network infrastructure devices that require management. This
presents a significant additional burden to the network
administration resources and is often a hurdle to adoption of
wireless technologies, particularly because the configuration of each
access point is nearly identical to the next. This near-sameness
often leads to misconfiguration and improper operation of the WLAN.

Second, distributing and maintaining a consistent configuration
throughout the entire set of access points in the WLAN is
problematic. Access point configuration consists of both long-term
static information (such as addressing and hardware settings) and
more dynamic provisioning information (such as individual WLAN
settings and security parameters). Large WLAN installations that
have to update dynamic provisioning information in all the APs in the
WLAN require a prolonged phase-over time. As each AP is updated, the
WLAN will not have a single, consistent configuration.

Third, dealing effectively with the dynamic nature of the WLAN medium
itself is difficult. Due to the shared nature of the wireless medium
(shared with APs in the same WLAN, with APs in other WLANs, and with
devices that are not APs at all), parameters controlling the wireless
medium on each AP must be monitored frequently and modified in a
coordinated fashion to maximize WLAN performance. This must be
coordinated among all the access points, to minimize the interference
of one access point with its neighbors. Manually monitoring these
metrics and determining a new, optimum configuration for the
parameters related to the wireless medium is a task that takes
significant time and effort.

Fourth, securing access to the network and preventing installation of
unauthorized access points is challenging. Physical locations for
access points are often difficult to secure since their location must
often be outside of a locked network closet or server room. Theft of
an access point, with its embedded secrets, allows a thief to obtain
access to the resources secured by those secrets.

Recently, to address some, or all, of the above problems, multiple
vendors have begun offering proprietary solutions that combine
aspects of network switching, centralized control and management, and
distributed wireless access in a variety of new architectures. Since
interoperable solutions allow enterprises and service providers a
broader choice, a standardized, interoperable interface between
access points and a centralized controller addressing the problems
seems desirable.

In currently fielded devices, the physical portions of this network
system are one or more 802.11 access points (APs) and one or more
central control devices, alternatively described as controllers (or
as access controllers, ACs). Ideally, a network designer would be
able to choose one or more vendors for the APs and one or more
vendors for the central control devices in sufficient numbers to
design a network with 802.11 wireless access to meet the designer's
requirements.

Current implementations are proprietary and are not interoperable.
This is due to a number of factors, including the disparate
architectural choices made by the various manufacturers. A taxonomy
of the architectures employed in the existing products in the market
will provide the basis of an output document to be provided to the
IEEE 802.11 Working Group. This taxonomy will be utilized by the
802.11 Working Group as input to their task of defining the
functional architecture of an access point. The functional
architecture, including descriptions of detailed functional blocks,
interfaces, and information flow, will be reviewed by CAPWAP to
determine if further work is necessary to apply or develop standard
protocols providing for multi-vendor interoperable implementations of
WLANs built from devices that adhere to the newly appearing
hierarchical architecture using a functional split between an access
point and an access controller.

3. Security Considerations

The devices used in WLANs control network access and provide for the
delivery of packets between hosts using the WLAN and other hosts on
the WLAN or elsewhere on the Internet. Therefore, the functions for
control and provisioning of wireless access points, require
protection to prevent misuse of the devices.

Confidentiality, integrity, and authenticity requirements should
address central management, monitoring, and control of wireless
access points that should be addressed. Once an AP and AC have been
authenticated to each other, a single level of authorization allowing
monitoring, control, and provisioning may not be sufficient. The
requirement for more than a single level of authorization should be

determined. Physical security should also be addressed for those
devices that contain sensitive security parameters that might
compromise the security of the system, if those parameters were to
fall into the hands of an attacker.

To provide comprehensive radio coverage, APs are often installed in
locations that are difficult to secure. The CAPWAP architecture may
reduce the consequences of a stolen AP. If high-value secrets, such
as a RADIUS shared secret, are stored in the AC, then the physical
loss of an AP does not compromise these secrets. Further, the AC can
easily be located in a physically secure location. Of course,
concentrating all the high-value secrets in one place makes the AC an
attractive target, and strict physical, procedural, and technical
controls are needed to protect the secrets.

Authors' Addresses

   Bob O'Hara
   Airespace
   110 Nortech Parkway
   San Jose, CA 95134

   Phone: +1 408-635-2025
   EMail: bob@airespace.com

   Pat R. Calhoun
   Airespace
   110 Nortech Parkway
   San Jose, CA 95134

   Phone: +1 408-635-2000
   EMail: pcalhoun@airespace.com

   James Kempf
   Docomo Labs USA
   181 Metro Drive, Suite 300
   San Jose, CA 95110

   Phone: +1 408 451 4711
   EMail: kempf@docomolabs-usa.com

Full Copyright Statement

   Copyright (C) The Internet Society (2005).

   This document is subject to the rights, licenses and restrictions
   contained in BCP 78, and except as set forth therein, the authors
   retain all their rights.

   This document and the information contained herein are provided on an
   "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
   OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET
   ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,
   INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE
   INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED
   WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the IETF's procedures with respect to rights in IETF Documents can
   be found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use of
   such proprietary rights by implementers or users of this
   specification can be obtained from the IETF on-line IPR repository at
   http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at ietf-
   ipr@ietf.org.

Acknowledgement

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