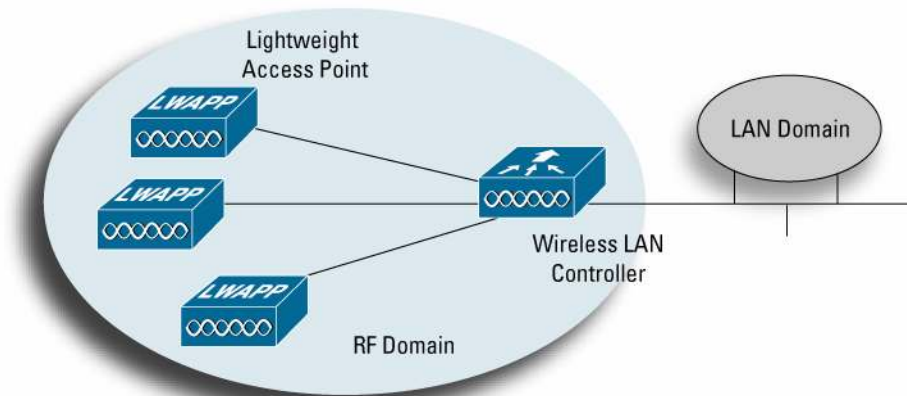


UNDERSTANDING THE LIGHTWEIGHT ACCESS POINT PROTOCOL (LWAPP)

There is a trend in the WLAN space toward centralized intelligence and control. In this new architecture, a WLAN controller system is used to create and enforce policies across many different lightweight access points. By centralizing intelligence within these devices, security, mobility, quality of service (QoS), and other functions essential to WLAN operations can be efficiently managed across an entire wireless enterprise. Furthermore, by splitting functions between the access point and the controller, IT staff can simplify management, improve performance, and increase security of large wireless networks.

Figure 1. Lightweight WLAN Systems Centralize Intelligence for Enterprisewide RF Management and Policy Control



As more vendors migrate to a hierarchical design, and as larger networks are built using lightweight access points, there is a need for a standardized protocol that governs how lightweight access points communicate with WLAN systems. This is the role of the Internet Engineering Task Force's (IETF's) latest draft specification, Lightweight Access Point Protocol (LWAPP). With LWAPP, large multivendor wireless networks can be deployed with maximum capabilities and increased flexibility.

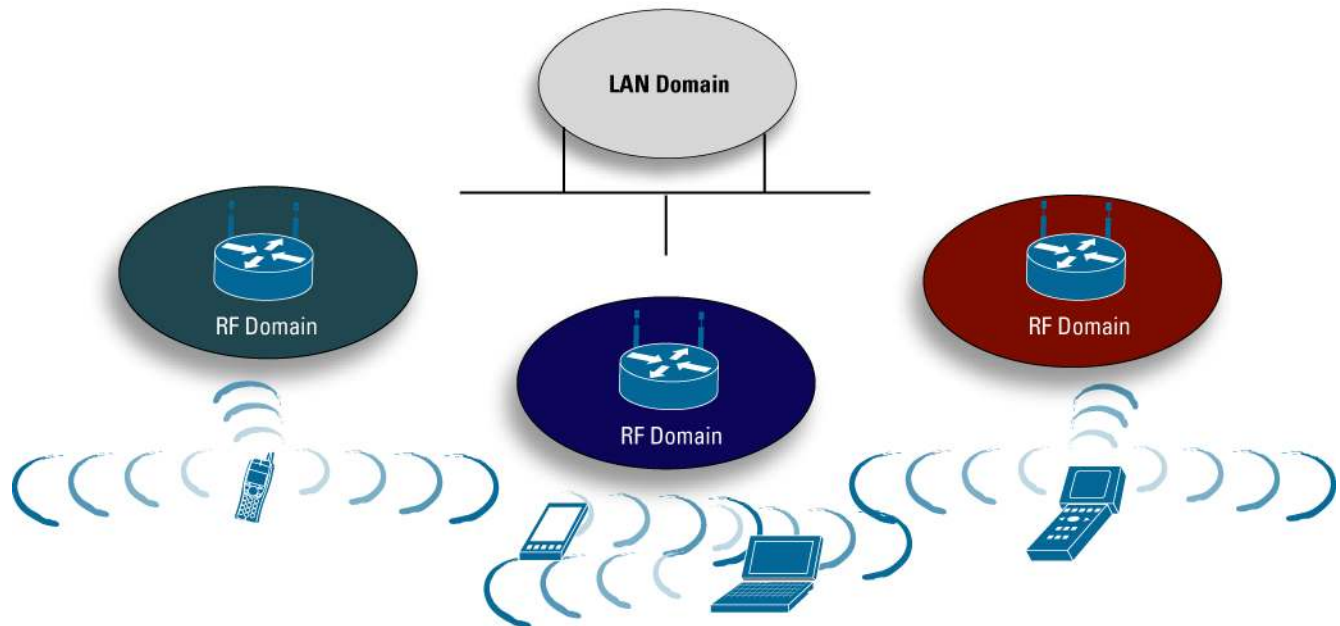
WHY A LIGHTWEIGHT ACCESS POINT?

Traditional WLAN solutions distribute all traffic handling, RF control, security, and mobility functions to the access point itself. However, this architecture limits visibility of 802.11 traffic to an individual access point only. This means:

- Individual access points, when used without a management device, must be managed individually, which can increase operations costs and staffing requirements
- Networkwide attacks and interference are not visible across a system
 - Single point of enforcement for security policies across Layer 1, Layer 2, and Layer 3
 - Unable to detect and mitigate denial of service (DoS) attacks across an entire WLAN
- A system cannot correlate or predict activity across an enterprise
 - Limits the ability to enable optimized, real-time load balancing
 - Clients cannot perform fast handoffs, which are required to support real-time applications such as voice and video

- There is an inherent security risk if an access point is stolen or compromised

Figure 2. Peer-to-Peer WLAN Architecture Limits Performance, Manageability, and Security



Numerous equipment vendors have responded to the limitations of a peer-to-peer WLAN architecture (Figure 2). Many of these vendors have announced new architectures that centralize WLAN intelligence for better performance and efficiency.

THE NEED FOR STANDARDIZATION

As more products emerge that use lightweight access points with centralized WLAN intelligence, there is a need for an industry standard that governs how these devices communicate with one another. The LWAPP is a draft being considered for standardization within the IETF working group to address this issue. Authored initially by Airespace (acquired by Cisco Systems in March 2005) and NTT DoCoMo, LWAPP standardizes the communications protocol between access points and WLAN systems (controllers, switches, routers, etc.). The goal of this initiative, as described in the IETF specification, is to:

- Reduce the amount of processing within an access point, enabling the limited computing resources within these devices to focus on wireless access, as opposed to filtering and policy enforcement
- Enable a scheme whereby traffic handling, authentication, encryption, and policy enforcement (QoS, security, etc) can be centralized for an entire WLAN system
- Provide a generic encapsulation and transport mechanism for multivendor access point interoperability, either by means of a Layer 2 infrastructure or an IP routed network

The LWAPP specification works to address these issues by defining the following types of activities:

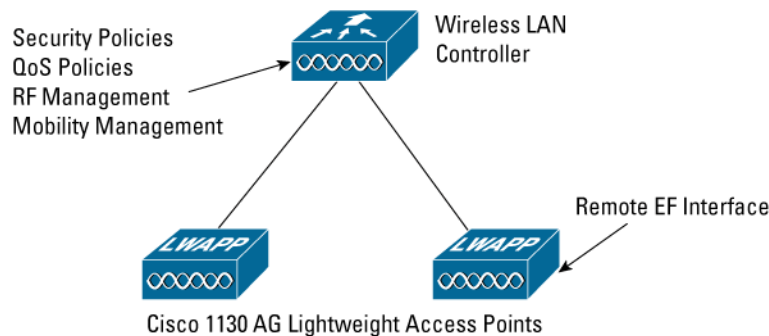
- Access point device discovery, information exchange, and configuration
- Access point certification and software control
- Packet encapsulation, fragmentation, and formatting
- Communications control and management between access point and wireless system device

Widespread LWAPP adoption would give enterprise customers choices in interoperable access points and wireless system devices, allowing them to make decisions based not on whether pieces of gear work together, but on the capabilities of individual access points and wireless system devices. Gaining industry acceptance of LWAPP will decrease single-vendor proprietary lock-in that requires that access points only be connected to their WLAN system devices to work optimally. LWAPP also provides an open standards solution for providing secure Layer 2 and Layer 3 networking services across multivendor centralized WLAN architectures. And with LWAPP, third-party vendors have a common architecture for application development.

PUTTING LWAPP TO WORK

When LWAPP was first introduced to the WLAN industry in 2002, it revolutionized the way WLAN deployments were managed with the concept of a “split MAC” the ability to separate the real-time aspects of the 802.11 protocol from most of its management aspects (Figure 3). In particular, real-time frame exchange and certain real-time portions of MAC management are accomplished within the access point, while authentication, security management, and mobility are handled by WLAN controllers. The Cisco Centralized WLAN Solution, which uses LWAPP, was the first centralized WLAN system to use the split MAC.

Figure 3. Cisco 1130 AG Lightweight Access Points



Combining LWAPP with Cisco’s intelligent RF management capabilities brings numerous benefits to customers.

Management

- Dynamic, systemwide RF management, including a host of features for smooth wireless operations, such as dynamic channel assignment, transmit power control, and load balancing.
- Single graphical interface for enterprisewide policies, including VLANs, security, and QoS.

Security

- Enterprisewide security policies that encompass all layers of a wireless network, from the radio layer through the MAC layer, and into the network layer. This makes it easier to provide uniformly enforced security and QoS or user policies that can address the particular capabilities of different classes of devices, such as handheld scanners, PDAs, or notebook computers.
- Discovery and mitigation of DoS attacks, and detection and denial of rogue access points. These functions occur across an entire Cisco Lightweight Wireless LAN Solution.

Mobility

- Cellular-like fast handoffs.
- Excellent support for real-time, mobile applications such as voice over WLAN.

LWAPP is an essential building block for business-critical wireless networks. It is a foundation upon which large-scale, heterogeneous WLANs can be constructed. By providing a standardized approach for RF internetworking, LWAPP protects companies' WLAN investments, simplifies RF management, and optimizes wireless networking for small, medium-sized, and large-scale WLAN deployments.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205327.CX_ETMG_LS_9.05