

Feature Brief: Wireless LAN High Availability for Remote Locations and Branch Offices



Challenge

Organizations are deploying wireless networks (WLANs) at remote locations and branch offices to connect to business partners, customers, employees, and assets anywhere, anytime. WLANs in remote locations facilitate real-time network access for mobile employees, equipment, and devices. They deliver business critical applications and mobility services that enable innovative applications, streamline business operations, improve productivity and enhance customer satisfaction.

Remote and branch office WLANs are being deployed to support retail stores, healthcare facilities, manufacturing plants, warehouses, educational locations, financial offices, local and national government organizations, and other remote locations worldwide.

With an increasingly distributed workforce, remote locations and branch offices require the same level of up time as headquarters locations. Network faults must be transparent to end users and network applications. Interruption of services delivered by the WLAN must be minimized. Business operations must continue, and access to business-critical applications such as voice communications, work-flow processes, location services, guest access, trading, and point of sales must be highly available and resilient.

Solution Overview

The [Cisco® Unified Wireless Network](#) addresses critical points of potential failure and helps enable resiliency and survivability for WLANs at remote locations and branch offices. This solution protects the WLAN by providing fast recovery from a variety of faults that may occur. With Cisco's high availability for remote WLANs, hardware and software work together to enable rapid recovery from disruptions and help ensure fault transparency to users and network applications.

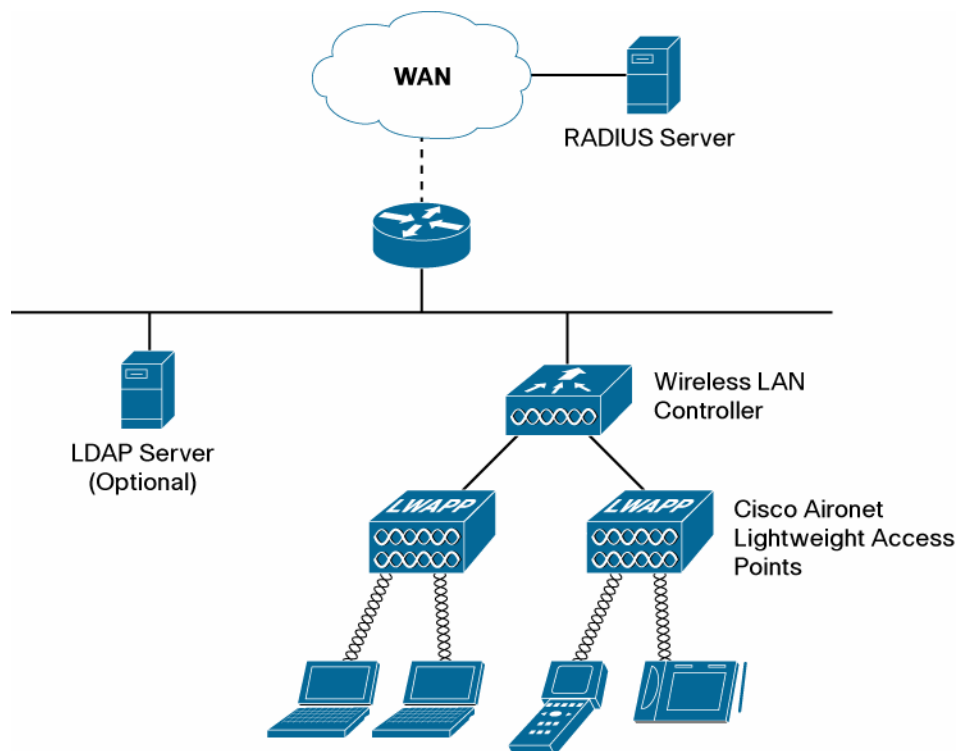
Features

The following features enhance the level of high availability offered by the Cisco Unified Wireless Network and are supported by [Cisco Aironet® lightweight access points](#) and [Cisco wireless LAN controllers](#) running Cisco Unified Wireless Network Software Release 4.2 and later. These features can be managed through the [Cisco wireless LAN controller](#) or [Cisco Wireless Control System \(WCS\)](#).

Local Extensible Authentication Protocol (EAP) Termination

Organizations that need a high level of reliability can enable EAP authentication through the local Cisco wireless LAN controller as a backup to authentication across the WAN link (Figure 1). This feature allows the wireless LAN controller to authenticate a local database of users without requiring a local RADIUS server. Users can be defined on the wireless LAN controller or in a Lightweight Directory Access Protocol (LDAP) database (for example, Microsoft Active Directory) that can be accessed by the wireless LAN controller. A variety of EAP types are supported, including: Protected Extensible Authentication Protocol (PEAP), Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), and Message Digest Algorithm 5 (MD5).

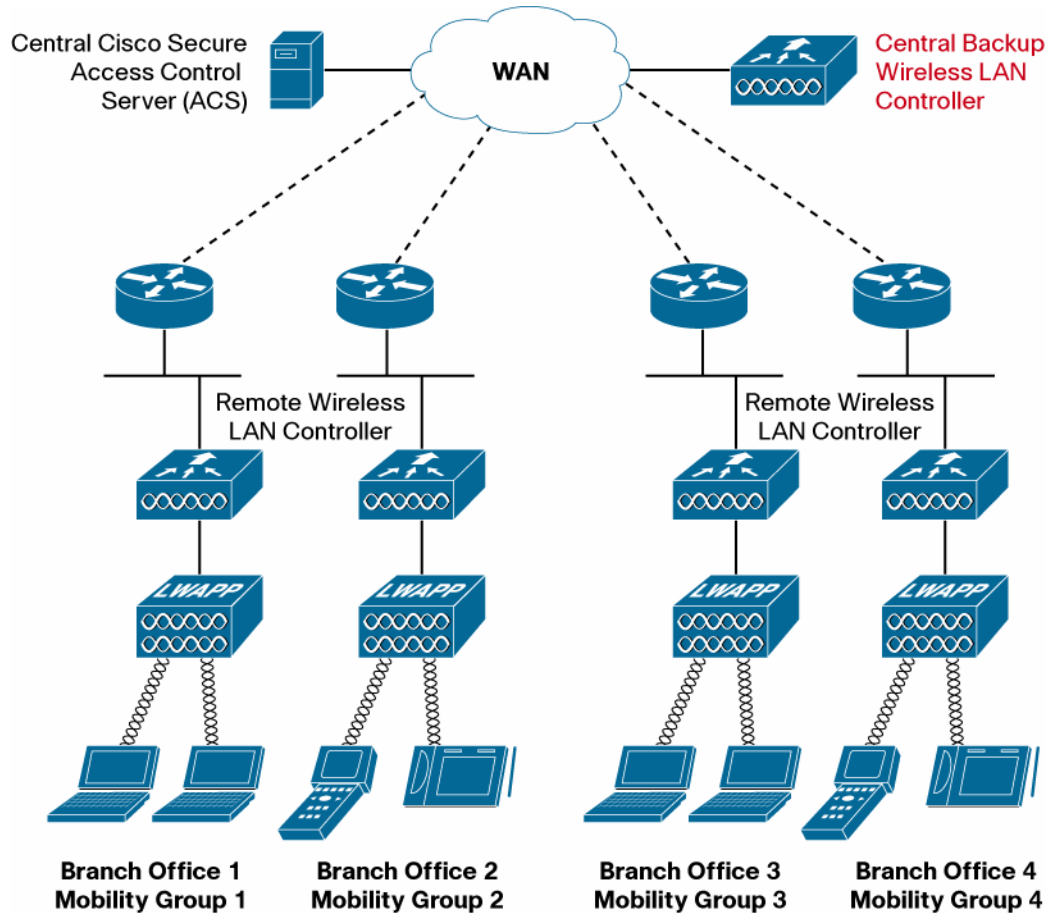
Figure 1. Local EAP Termination



Centralized Wireless LAN Controller Back Up for Multiple Remote Locations

A single Cisco wireless LAN controller at a centralized location can now act as a backup for remote wireless LAN controllers across mobility groups (Figure 2). This greatly simplifies global provisioning and lowers capital expenses by reducing the number of backup wireless LAN controllers required. It also delivers centralized redundancy for failover and rapid recovery from a remote wireless LAN controller hardware failure, operating system failure, or power failure. A secondary controller is recommended when local redundancy is required.

Figure 2. Centralized Wireless LAN Controller Back Up for Multiple Remote Wireless LAN Controllers



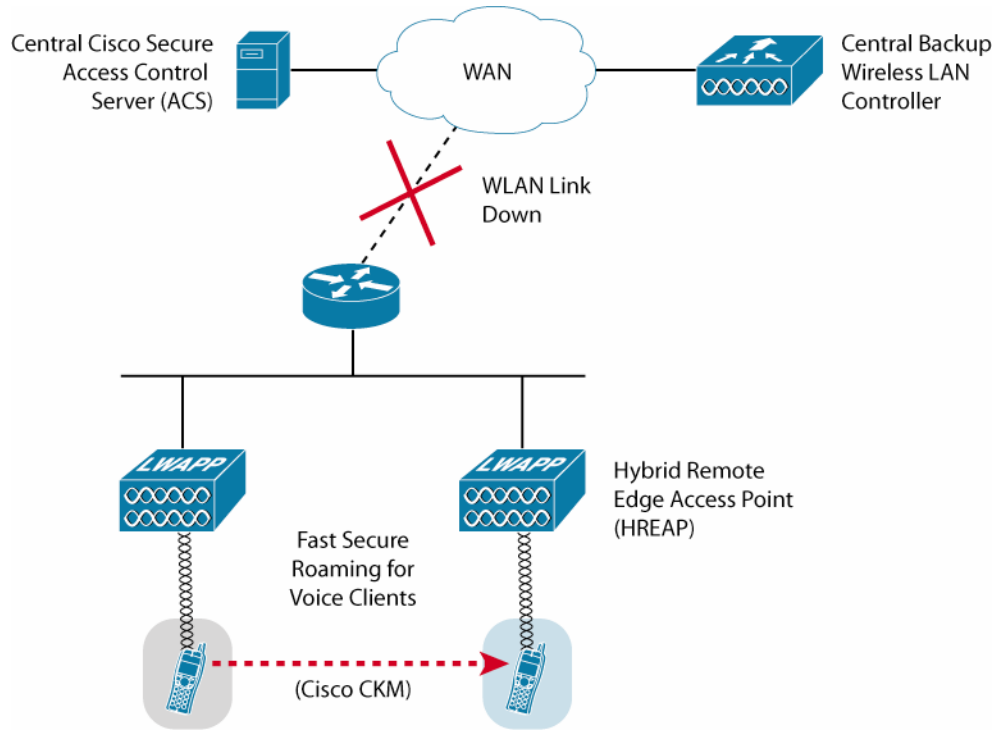
Hybrid Remote Edge Access Point (HREAP) for Remote Locations

Organizations can provide wireless LAN services to remote and branch offices without deploying a wireless LAN controller at each location by deploying an HREAP that is configured and controlled centrally through a wide area network (WAN) link. HREAPs facilitate unified enterprise-wide wireless LAN services and support centralized control of Service Set Identifiers (SSIDs), security parameters, and software loads. With an HREAP, organizations can choose to bridge traffic locally, tunnel traffic over the WAN, or tunnel traffic over LWAPP on a per-SSID basis. HREAPs provide organizations with more flexibility in setting up wireless access at remote locations. An unlimited number of HREAPs can be deployed at each location, but the WAN link must support a minimum speed of 128-kbps WAN throughput and 100-ms maximum roundtrip latency between each HREAP and the centralized wireless LAN controller.

HREAP Support for Cisco Centralized Key Management (CKM)

Remote voice clients that are connected to an HREAP and are using Cisco Centralized Key Management (CKM) will stay connected to the network as they roam between local HREAPs, even if the WAN link is lost (Figure 3). This feature facilitates reliable voice services for remote sites that rely on voice communications for real-time business operations.

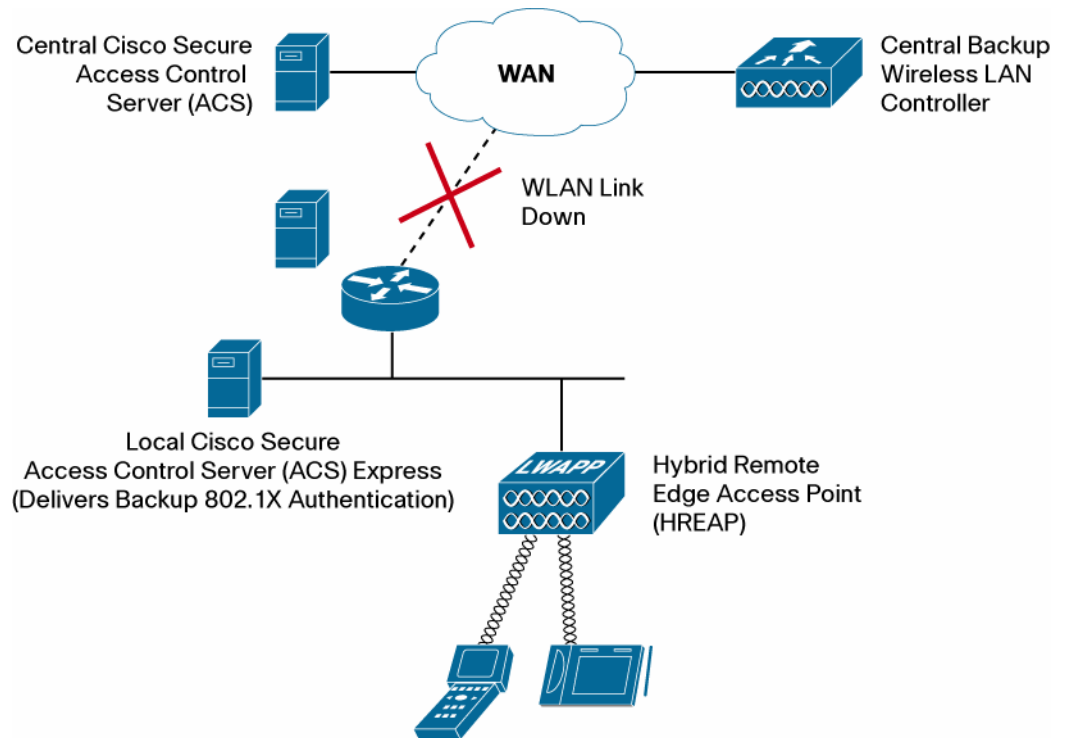
Figure 3. HREAP Support for Cisco Centralized Key Management



HREAP Support for Local IEEE 802.1X Authentication

Organizations can now locally authenticate clients in remote locations during a WAN outage using an HREAP and a local authentication, authorization, and accounting (AAA)/RADIUS server (Figure 4). Both new clients joining the WLAN, and existing clients that are re-authenticated, can be authenticated locally via the HREAP. This feature enables resilient IEEE 802.1X authentication for remote client devices, enabling transparent WLAN access for end users even when the WAN link is down.

Figure 4. HREAP Support for Local IEEE 802.1X Authentication



Benefits

The benefits of high availability to organizations deploying the Cisco Unified Wireless Network at remote locations and branch offices include the following:

- Reduced total cost of ownership through centralized wireless LAN controller redundancy that supports failover of remote wireless LAN controllers
- Scalable simplified WLAN management of all central and worldwide remote locations from an easily accessible centralized management console
- Real-time wireless access to business-critical applications for remote users
- Simplified security management with support for local or centralized user authentication
- Built-in secure guest access for all remote locations
- Improved voice over WLAN call management and reduced call loss for roaming voice client devices
- Real-time location tracking for remote locations from Cisco location services

Solution Components

- Cisco Unified Wireless Network
- Cisco Aironet Access Points (Configured as HREAP)
- Cisco Wireless LAN Controllers
- Cisco Wireless Control System (WCS)

Summary

The Cisco Unified Wireless Network delivers resiliency and survivability for WLANs at remote locations and branch offices. It supports rapid recovery from network disruptions and helps ensure fault transparency to users and network applications. Service interruptions are minimized and high availability is delivered for remote WLANs through the Cisco Unified Wireless Network.



Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (63637)
 Fax: 408 527-0689

Asia Pacific Headquarters
 Cisco Systems, Inc.
 16B Robinson Road
 #29-01 Capital Tower
 Singapore 068912
www.cisco.com
 Tel: +85 6317 7777
 Fax: +85 6317 7769

Europe Headquarters
 Cisco Systems International BV
 Heisterbergpark
 Heisterbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www-europe.cisco.com
 Tel: +31 0 20 620 6791
 Fax: +31 0 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Green Route Bridge logo are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play and Learn is a service mark of Cisco Systems, Inc.; and Access, Registrar, Aironet, BPX, Catalyst, CCNA, CCIP, CCIE, CCI, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solved, EtherChannel, EtherFast, EtherSwitch, Fast, Step, Follow Me, Browser, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, IPPhone, IPTV, IQ Experience, the IQ logo, IQ Net, RealTime Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (070509)