Wireless LAN Support for the Cisco 860 and 880 Series Integrated Services Routers

WLAN Feature Overview

Q. How do the Cisco® 860 and 880 Series Integrated Services Routers support wireless LAN?

A. The Cisco 860 and 880 Series uses an embedded access point to provide 802.11n wireless LAN capabilities in the 2.4-GHz frequency range using integrated multiple-input, multiple-output (MIMO) technology. This provides higher throughput and more reliability for the wireless environment.

Q. How does the embedded access point in the Cisco 860 and 880 Series fit into Cisco's WLAN product portfolio?

A. The embedded access point uses the same software release train images as the existing Cisco Aironet® access point product family and shares similar features and feature roadmap. It can operate in either standalone (autonomous) or unified mode (Cisco 880 Series only). When running in unified mode, the embedded access point becomes a node on the wireless network and is supported by the full range of wireless LAN controllers and the Cisco Wireless Control System (WCS). Hence, it can take advantage of the unified feature set, which includes guest access, wireless intrusion detection and intrusion prevention, and Layer 3 mobility.

Q. What wireless LAN standards are supported on the Cisco 860 and 880 Series routers?

A. The Cisco 860 and 880 Series supports the standard IEEE 802.11b/g as well as IEEE 802.11n draft 2.0 and is Wi-Fi 802.11n draft 2.0 certified.

Q. What are the primary differences between the wireless LAN support on the Cisco 850 and 870 Series Integrated Services Routers and the Cisco 860 and 880 Series?

A. The Cisco 860 and 880 Series offers higher wireless throughput with the support for 802.11n and MIMO with the use of multiple antennas. These routers are shipped with three captive omnidirectional antennas by default. The embedded access point in the Cisco 860 and 880 Series runs a separate image from the host router and can operate in either autonomous or unified (Cisco 880 Series only) mode.

Q. What client devices are compatible with the Cisco 860 and 880 Series embedded access point?

A. The Cisco 860 and 880 Series embedded access point is interoperable with any 802.11n draft 2.0, 802.11b, or 802.11g Wi-Fi-certified clients. Cisco clients and third-party Cisco Compatible Extensions clients can take advantage of the enhanced capabilities provided by the access point.

WLAN Feature Details

Q. Is the Cisco 880 Series orderable with unified mode already enabled?

A. Customers that purchase directly from Cisco can configure this when placing the order with the Cisco Dynamic Configuration Tool. Cisco 880 Series routers sold through distribution will have autonomous mode enabled by default with the option for migrating to unified mode.

Q. Are the embedded access points upgradable to unified mode in the field?

A. Yes, the access points deployed in autonomous mode may later be upgraded in the field to unified mode. See the requirements directly below.

Q. What is required to operate the embedded access point in unified mode?

A. Unified mode is supported on the Cisco 880 Series only. The host router must have the Advanced IP Services feature set in order to enable unified mode for the embedded access point. The access point's boot image type must be configured on the host router to enable unified mode. After this enable command-line interface (CLI) is invoked, the access point must be rebooted in order to go to unified mode. Make sure that the wireless LAN controller is running version 5.1 or later.

Q. How is the software on the embedded access point upgraded?

A. The embedded access point runs a separate image from the host router, so the access point image can be upgraded without affecting the host router. The embedded access point is shipped by default with the autonomous image (AP801-k9w7) as well as a recovery image (rcvk9w8) that allows upgrade to unified mode. See online documentation on how to upgrade the access point software.

Q. How is the embedded access point managed and configured?

A. If the access point is operating in autonomous mode, there are a few methods to configure it:

- If this is an initial configuration, Cisco Configuration Professional Express (Cisco CP Express) allows minimal configuration such as a Secure Set Identifier (SSID) and encryption for a single SSID.
- For more advanced configurations, a GUI is available at http://x.x.x.x, where x.x.x.x is the IP address of the access point’s management interface (BVI).
- The CLI on the access point is also available for configuration by initiating a session from the host router using the CLI “service-module wlan-ap 0 session.”
- If the access point is operating in unified mode, the wireless LAN controller offers a GUI to configure the access point.

Q. What is H-REAP mode?

A. Hybrid Remote Edge Access Point (H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a WAN link without deploying a controller in each office. The H-REAP access point can switch client data traffic locally and perform client authentication locally when the connection to the controller is lost. When connected to the controller, access points running H-REAP can also tunnel traffic back to the controller. Most security features on either centrally or locally switched WLANs work, provided the path between the H-REAP and the controller is up. When this link is down, only a subset of these security options allow new clients to connect to locally switched WLANs. See the H-REAP design and deployment guide for more detailed information. H-REAP is only available with unified mode; hence it is not supported on the Cisco 860 Series access point.

Q. Does the embedded access point support link role flexibility?

A. When operating in autonomous mode, the embedded access point supports access point, root bridge, non-root bridge, and workgroup bridge.

Q. Which wireless LAN security features are available on the embedded access points?

A. The embedded access points support standards-based authentication and encryption,

including support for 802.11i, Wi-Fi Protected Access (WPA), WPA2, and numerous Extensible Authentication Protocol (EAP) types. These certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and Advanced Encryption Standard (AES) for WPA2 encryption. Note that when TKIP and WEP are configured on the radio interface, only speeds of up to 802.11g can be achieved.

Q. Is wireless quality of service (QoS) supported on the Cisco 860 and 880 Series access points?

A. The embedded access point supports Wi-Fi Multimedia (WMM), a QoS system based on the IEEE 802.11e draft that has been published by the Wi-Fi Alliance. WMM is enabled by default on access points operating in autonomous mode. For WMM support in unified mode, see the configuration guide for wireless QoS on the wireless LAN controllers.

Q. How many SSIDs and wireless VLANs are supported on the Cisco 860 and 880 Series embedded access point?

A. The embedded access point supports 16 SSIDs, MBSSIDs, and VLANs on the radio interface. In order to enable inter-VLAN routing on the host router for the VLAN traffic coming from the access point, the number of VLANs supported on the host router needs to be taken into consideration. See the Cisco 860 and 880 Series data sheet for more information on the number of VLANs supported.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**

Printed in USA C67-458884-00 03/08