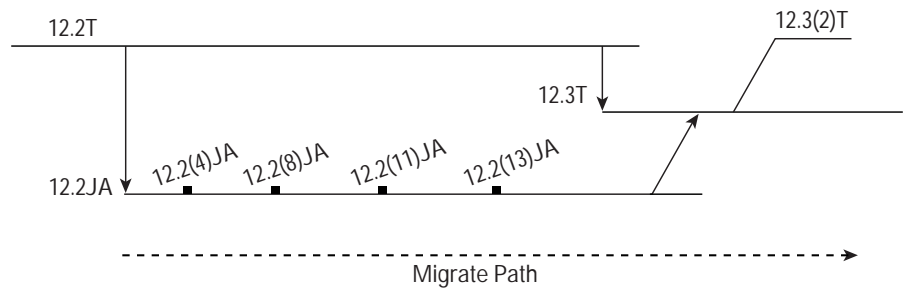


Cisco IOS Deployment Release 12.2(4)JA

This product bulletin describes the content and delivery information concerning Cisco IOS® Software Release 12.2(4)JA. This release is specific for the Cisco Aironet® 1100 Series platform. For more information about the Cisco IOS Software release process, see Product Bulletin 537.

Migration Guide

Figure 1 displays Cisco IOS 12.2(4)JA release functionality relative to the 12.2T release. This figure also identifies the recommended migration path.



New Features in 12.2(4)JA

Cisco IOS Release 12.2(4)JA is the first release that supports Cisco Aironet wireless infrastructure platforms. This release supports the Cisco Aironet 1100 Series platform.

Table 1 gives the new features that are supported in the initial release of 12.2(4)JA.

Table 1 Cisco IOS Release 12.2(4)JA Features

New Features
Wireless
802.11 wireless standards
Inter-access point roaming
Multiple service set identifiers (SSIDs)
World mode
Configurable radio transmit power
Link diagnostics



Table 1 Cisco IOS Release 12.2(4)JA Features (Continued)

New Features
Networking
Transparent bridging
Virtual LANs (VLANs)
Quality of service (QoS)
Proxy Mobile IP
Hot standby
Load balancing
Management
Hypertext Transfer Protocol (HTTP) server
Management Information Bases (MIBs)
Access control lists
Cisco Wireless Security Suite
802.1X, Extensible Authentication Protocol (EAP)
Key hashing
Message integrity check (MIC)
Broadcast key rotation

Detailed Information

802.11 Wireless Standards

This feature provides support for IEEE 802.11 standards for wireless networking. It enables interoperability under 802.11 specifications for network architecture, wireless association, and radio management. It includes support for management of mode of operation (access point or repeater), Service Set Identifier (SSID), authentication type, channel selection, transmission rates, power-save mode, and wired equivalent privacy (WEP)-based security, among other configurable fields.

Inter-Access Point Roaming

Clients who roam from one access point to another are supported with pre-standard services for seamless hand-off defined under IEEE 802.11f Inter-Access Point Protocol (IAPP). With this feature, when a client roams from a first access point to a second one, the second access point sends a message to the first to update its association table, establishing a learning path to the client for the switch. This feature provides backward compatibility with the Cisco Aironet Data Delivery Protocol for inter-access point hand-off as implemented on the Cisco Aironet 340, 350, and 1200 Series.



Multiple SSIDs

With this feature, an access point can support up to 16 SSIDs, enabling flexible service deployment. Each SSID can be configured based on several parameters, creating up to 16 unique sets of services. Configurable parameters include mode for guest clients (enabling broadcasted SSID), client authentication method, maximum number of client associations, VLAN identifier, proxy mobile IP enabled, Remote Access Dial-In User Service (RADIUS) accounting list identifier, and SSID designate in repeater mode.

World Mode

Each country regulates usage of the 2.4-GHz spectrum in its domain with respect to channel availability and allowable transmit power. The world mode feature automates client configuration of channel and transmit power settings by allowing world mode-enabled infrastructure devices to configure the capabilities of world mode-enabled clients. Users who travel with their wireless client between countries and specify differing sets of regulations can use the same client cards in world mode-enabled deployments.

Configurable Radio Transmit Power

The transmit power of the access point radio can be configured from 1 mW up to 100 mW. This allows customers to manipulate the coverage area provided by the access point consistent with their needs.

Link Diagnostics

This feature provides testing and diagnosis capabilities of the wireless interface for connectivity status and throughput performance. The network administrator can examine radio configuration information such as the operating channel, transmit power, supported data rates, and regulatory settings; run a link test; determine signal strength and quality; diagnose the client association and authentication process; and examine data packets sent over wireless.

Transparent Bridging

The access point bridges the network between the wired infrastructure and wireless devices, switching traffic between the radio frequency and Ethernet interfaces. This feature provides transparent bridging and forwarding logic between these interfaces.

VLAN over Wireless

VLANs allow a network to be partitioned into logical subnets that are independent of physical location. This allows services, such as network access, to be differentiated by user. This feature defines 802.1q VLANs for wireless LANs, using a VLAN identifier in the Ethernet frame. Up to 16 VLANs, one per SSID, are supported in this release.

QoS over Wireless

This feature enables the access point to provide traffic prioritization services over the wireless interface for standards-based quality of service (QoS). This feature prioritizes traffic based on the 802.1p tag in the Ethernet header or the IP type of service/Differentiated Services Code Point (TOS/DSCP) bits in the IP header.



Proxy Mobile IP

This release supports the Proxy Mobile IP protocol for seamless inter-subnet roaming. With Proxy Mobile IP, when a client roams from one subnet to the next, the client's IP address and session are maintained. The access point is a mobile IP proxy for clients who do not have the mobile IP software installed in the device. The access point informs the foreign agent router that the client has roamed to another subnet, while the foreign agent directs the home agent to reroute packets to it.

Hot Standby

Higher wireless network availability can be achieved by installing a standby access point as a backup for a primary device and configuring it for hot standby. When installed on the same Ethernet LAN and configured consistently as a primary device, the standby device associates to the primary device as a client and monitors the primary device with periodic link test request packets sent over both the Ethernet and wireless interfaces. The standby device assumes the role of access point by activating its Ethernet port and accepting radio client associations if the primary device fails to respond with a link test response packet.

Load Balancing

The load-balancing feature optimizes aggregate bandwidth with intelligent user associations, resulting in a better load distribution. At initialization, the client polls all access points within range for the device load information, and selects the one with the lightest load. With this feature, the access point interprets the request and provides information to the client.

HTTP Server

This feature enables Web-based graphical user interface (GUI) management by providing support for HTML Web pages and Common Gateway Interface (CGI) scripts using common Web browsers.

MIBs

This release provides support for standard and Cisco Enterprise MIB I and MIB II. New MIBs for wireless are defined in this release. More information on the supported MIBs is available at:

- <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Access Control Lists

Access control lists allow filtering of traffic based on identifiable attributes within an Ethernet frame. Data can be filtered based on source or destination addresses, protocol used, protocol-specific options (Telnet, File Transfer Protocol [FTP], HTTP, Simple Network Management Protocol [SNMP]), and Media Access Control (MAC) address.



802.1X, EAP

This Cisco Wireless Security Suite feature supports the 802.1X standard port-based authentication framework including EAP Cisco Wireless (LEAP), Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol Transport Layer Security (EAP-TLS) and EAP-Tunneled TLS (EAP-TTLS).

Key Hashing

With this pre-standard implementation of the key hashing technique, the base key and packet-unique initialization vector are hashed together to create a new, per-packet key. This procedure mitigates those passive attacks that attempt to determine the base key by accumulating enough weak initialization vectors. Key hashing is a component of the Cisco Wireless Security Suite pre-standard Temporal Key Integrity Protocol (TKIP), which is part of the draft for IEEE 802.11i enhanced wireless security.

Message Integrity Check

This feature supports a pre-standard implementation of the Message Integrity Check (MIC) protocol. With this feature, the access point validates that packets received from the client have not been tampered with by calculating the packet checksum and comparing it to the checksum calculated and sent by the client. This feature prevents active attacks such as bit-flipping attacks. MIC is also a component of the Cisco Wireless Security Suite pre-standard TKIP.

Broadcast Key Rotation

This Cisco Wireless Security Suite feature enables the network administrator to set the shared broadcast key to timeout, causing a new broadcast key to be generated. This procedure mitigates passive attacks attempting to determine the broadcast key from weak initialization vectors.

Platform Support

The Cisco Aironet 1100 Series platform consists of the AP1120B - 802.11b access point with integrated antennas.

Detailed Information

For more information about the features being delivered in 12.2(4)JA, reference the following release notes documents:

- http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_release_notes_list.html

Product Numbers

Cisco IOS Software Release 12.2(4)JA feature set, images, and memory recommendations are given in Table 2:

Table 2 Memory Recommendations for Cisco IOS Release 12.2(4)JA

Platform	Software feature set	Product code	Image	Flash	DRAM
AP1120B	Wireless	S11W7K9-12204JA	c1100k9w7.tar-122-4JA	8	16

Download Information

Customers can download Cisco IOS Release 12.2(4)JA Software from Cisco.com in the Software Image Library.

- <http://www.cisco.com/public/sw-center/sw-ios.shtml>
- <http://www.cisco.com/public/sw-center/sw-wireless.shtml>



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0208R)