# Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Wireless LAN Services Module Software Release 2.1.1

**Current Release: 2.1.1—March 3, 2006**

This publication describes the features, modifications, and caveats for the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module (WLSM) software release 2.1.1.

**Note** For installation and configuration procedures for the WLSM, refer to the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module documentation at this URL:

http://www.cisco.com/en/US/products/index.html

## Contents

This document consists of these sections:




**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# System Requirements

This section describes the system requirements for the Catalyst 6500 series and Cisco 7600 series WLSM software release 2.x:



## Hardware Requirements

The wireless LAN software requires the following hardware:

- Catalyst 6500 series switch or Cisco 7600 series router
- Supervisor Engine 720
- Catalyst 6500 series and Cisco 7600 series WLSM

## Software Requirements

Table 1 lists the wireless LAN software versions supported by Cisco IOS software.

***Table 1 Wireless LAN Software Compatibility***

| Product Number | Minimum WLAN Software Version | Recommended WLAN Software Version | Minimum Cisco IOS Software | Recommended Cisco IOS Software |
|---|---|---|---|---|
| WS-SVC-WLAN-1-K9 with Supervisor Engine 720 | • Application Image: 1.1(1)<br>• Maintenance Image: 3.1(1) | • Application Image: 2.1.1<br>• Maintenance Image: 3.1(1) | Cisco IOS Software 12.2(18)SXF2 supports WLSM image 2.1(1) | • Supervisor Engine 720: 12.2(18)SXF2<br>• Access points: 12.3(8)JA |

## Solution Requirements

In addition to the hardware and software requirements, the WLSM also requires the following:

- Cisco Aironet 1100, 1130AG, 1200, 1230AG, and 1240AG Series Access Points and Cisco Aironet 1300 Series Outdoor Access Point/Bridge using Cisco IOS Release 12.2(15)XR or Release 12.3(2)JA or later, Cisco Aironet 1130 Series Access Point using Cisco IOS Release 12.3(2)JA or later, or Cisco Aironet 1310 Outdoor Access Point/Bridge (configured in access point mode) using Cisco IOS Release 12.3(2)JA or later
- CiscoWorks Wireless LAN Solution Engine (WLSE) release 2.7(1) or later

# Orderable Software Images

Table 2 lists the software releases and applicable ordering information for the wireless LAN software.

*Table 2 Orderable Software Images*

| Software Releases | Filename | Orderable Product Number |
|---|---|---|
| 2.1.1 | c6svc-wlan-k9w7.2.1.1.bin | SWLSMW7K9-21 |

# Features in Software Release 2.1.1

This section describes the features available in wireless LAN software release 2.1.1:

- Increased access point scalability—Memory and software improvements increase scalability of Cisco Catalyst 6500 Series WLSM from 300 to 600 access points per WLSM.
- Active and standby WLSMs per chassis—Active and standby WLSMs in a common Cisco Catalyst 6500 Series chassis provide the ability for administrators to deploy a second WLSM in a given chassis for failover support. One WSLM serves in an active role, the other WLSM serves in a standby role at any given time.
- Resilient Tunnel Recovery—Automatic recovery of mobility tunnels after WLSM failure with zero client interruption.
- RADIUS-based mobility group assignment—This feature provides the ability to assign wireless users to different mobility groups based on user credentials stored in the RADIUS server.
- IGMP snooping-based multicast for wireless—This feature provides the ability to deliver multicast traffic to wireless clients across the Native VLAN of an access point without requiring the need for trunking or multiple multicast enabled networks on the first hop layer 3 router. With this feature, the access point is able to deliver multicast to wireless clients with dynamically assigned mobility groups.
- Support for 240 mobility groups—This feature increases the number of mobility groups that may be assigned per WLSM. Mobility groups may be dynamically assigned based upon user authentication or posture validation. With 240 mobility groups supported per WLSM, each mobility domain may be smaller, thus reducing the subnet size required for each mobility group.
- Enhanced Cisco Catalyst WLSM MIB support—MIB support (CISCO-WDS-INFO-MIB) introduces the capability of querying the Cisco Catalyst 6500 series WLSM for client, access point, and WLSM configuration and statistics. This information may be used to query the WLSM for client association, roaming, and performance data via the CiscoWorks Wireless LAN Solution Engine (WLSE) or custom Simple Network Management Protocol (SNMP) applications.

# Features in Software Release 1.x

For a complete list of features for WLSM software releases 1.x, refer to the *Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Wireless LAN Services Module Software Release 1.x* at this URL:

http://www.cisco.com/en/US/products/index.html

# Limitations and Restrictions

This section describes general limitations and restrictions:

- In software release 1.1.1 through 1.4.1, you can install one WLSM in a chassis.
- In software release 2.1.1, you can install two WLSMs, which requires Cisco IOS Release 12.2(18)SXF2.
- You cannot configure wireless clients in the same subnet as wired clients.
- You cannot map multiple SSIDs to a single network ID.
- You cannot configure QoS on tunnel interfaces in systems with a PFC3A. There is full QoS support in systems with a PFC3B or PFC3BXL.
- If you upgrade your Supervisor 720 to Cisco IOS Release 12.2(18)SFX2, you must be running Cisco Wireless LAN Services Module software version 1.4.3 or greater on your WLSM.

# Documentation Updates

- The *Cisco Catalyst 6500 Series Wireless LAN Services Module: Detailed Design and Implementation Guide* contains an incorrect entry pertaining to default gateway IP addresses

  The WLSM Failover—The "DHCP Configuration" section on page 56 states that the DHCP server must be configured to return both IP address to the client. This is not correct because the specific default gateway that a client uses is ignored by the access point and all traffic is sent to the upstream tunnel address. The tunnel address changes after the access point registers with the backup WDS and new tunnels are created by its corresponding Supervisor 720 module. Only one gateway is needed.

  This discrepancy is documented in open caveat CSCej53619.

# Open and Resolved Caveats in Software Release 2.1.1

These sections describe open and resolved caveats in wireless LAN software release 2.1.1:


- Open Caveats in Release 2.1.1, page 4
- Resolved Caveats in Release 2.1.1, page 7


## Open Caveats in Release 2.1.1

This section describes open caveats for the wireless LAN software release 2.1.1:

- CSCsc05022—High CPU workaround for 240 mobility routing configuration

  When a large number of mGRE tunnels are configured on the Supervisor 720 as part of the 240 mobility support feature, a large number of advertisements occur from the routing protocol. The advertisements can cause a high CPU utilization rate, which results in reduced performance.

  To help alleviate this problem, first turn off all router protocol advertisements using the router's **passive-interface default** command. Then specify interfaces, VLANs, and networks for which you want advertisements to be broadcast.

The following table shows this workaround for EIGRP:

| Command | Remarks |
|---|---|
| **router eigrp** | Designates router protocol to address. |
| **passive-interface default** | All interfaces will not send EIGRP advertisements. |
| **no passive-interface** *interface* | Enter for all physical interfaces for which you want advertisements sent so that neighbors are formed and routes exchanged. |
| **no passive-interface** *vlan* | Enter for all VLANs to which EIGRP advertisements should be sent. |
| **network** *x.x.x.x* | Include all tunnel interfaces with a separate **network** command. Also include other networks that need to be advertised. |

- CSCsg46103—The WLSM does not support DHCP snooping for MPLS tags sent from the supervisor engine to the access point.

  **Workaround**: In networks where the access point sends traffic to the WLSM across an MPLS cloud (for example, AP–>SW1–>MPLS CLOUD–>SW2–>WLSM), remove the MPLS label that is sent to the WLSM by disabling the MPLS label advertisement for the access point subnet on the next hop MPLS-router to the WLSM by entering the following commands on the supervisor engine on SW1.

  ```
  access-list access-list number deny ip_addr ap_subnet_ip_addr
  access-list access-list number permit any

  mpls ldp advertise-label oldstyle
  mpls ldp advertise-label for access-list number
  ```

  This workaround is not necessary if the access point is connected to an MPLS penultimate hop popping (PHP) switch (AP--SW1--SW_WLSM); the SW_WLSM does not see MPLS-encapsulated IP traffic from the access point.

- CSCsb54133—Some Radius Assigned Clients cannot associate if the access point has 16 VLANs configured.

  The following system log message is displayed on the console when all the dot11 VLAN resources are exhausted:

  ```
  %DOT11-4-WLAN_RESOURCE_LIMIT: WLAN Limit exceeded on interface Dot11Radio0 and
  Network-id101
  ```

  This message is followed by an authentication failure message:

  ```
  %DOT11-7-AUTH_FAILED: Station 0001.0001.0001 Authentication failed
  ```

  The access point de-authenticates the dynamic client because it has limited VLAN resources on the access point. The administrator must make sure that there are VLANs left over on the access point for dynamic networks assigned by the AAA server. The access point currently supports a maximum of 16 VLANs. Each dynamic network (not statically configured on the access point) will need one VLAN resource.

- CSCsb94219—Mobile node does not associate with the 16th SSID when one of the 16 SSIDs is not mapped to VLAN 1.

The access point requires VLAN 1 when 802.1Q trunking is enabled. Unfortunately, when 16 SSIDs are configured on an access point, and one of 16 SSIDs is not mapped to VLAN 1, association with the 16th SSID fails. However, association with the other 15 SSIDs will succeed because VLAN 1 must be enabled, one VLAN resource is consumed, causing the 16th SSID to be disabled.

- CSCej60290—If a user sets the WLSM recovery timer to 0 seconds (disable-recovery) while a WLSM recovery is already in progress, the recovery is not affected. However, if the user performs an SSO, the recovery in progress stops.

  If an SSO is performed during a WLSM graceful recovery, the WLSM graceful recovery process starts again in the new active Supervisor 720 using the current recovery timer value. If the user sets the timer to 0 seconds, and then performs an SSO switchover, the new active Supervisor 720 attempts to start a WLSM recovery from the currently set value. Because the value is now 0, the graceful recovery stops.

  This behavior is according to design.

- CSCej63681—Tunnel state remains up in both Catalyst 6500 switches when back-to-back WLSM failures occur, which could result in a disruption of wireless data traffic.

  In the rare occurrence where both WLSMs in a single switch fail in quick succession and the switch stays up, the switch may not be aware of backup WLSMs on another switch. If this occurs, both switches advertise a route to the subnets for mobile nodes, which has the potential for disrupting traffic forwarding.

  The problem does not occur in a single switch, two-WLSM configuration because a graceful recovery begins if both WLSMs fail back-to-back.

- CSCsb59039—Only BSS mode is supported when a workgroup bridge associates to Layer 3 mobility over WLSM WDS.

  Infrastructure mode is not supported when a workgroup bridge associates to Layer 3 mobility over WLSM WDS. In this mode, the workgroup bridge and its clients are able to associate to the root access point on an SSID with a mobility ID. However, the workgroup bridge and clients fail to pass traffic and obtain a DHCP address.

  Infrastructure mode is supported when a workgroup bridge associates to Layer 2 over WLSM WDS. In this case, no mobility group is configured on an SSID and no RADIUS tunnel assignment is established on ACS for workgroup bridge clients.

- CSCsc21693—RPR active Supervisor generates crashinfo when shutting down.

  When the **redundancy force-switchover** command is executed on the Catalyst 6500 switch active Supervisor 720 to perform an RPR switchover, the Supervisor 720 may dump debug information and display warning messages similar to the following:

  ```
  %CPU_MONITOR-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 30 seconds
  [5/0]
  Writing crashinfo to bootflash: debuginfo_2005018-081422
  ```

  This does not create a problem because the new active Supervisor 720 is not affected and the old active Supervisor 720 is being shut down.

  The symptom may be seen only when there is a service module such as a WLSM present in the Catalyst 6500 chassis and an RPR switchover is performed.

  There is no workaround for this situation.

- CSCsc46281—%PM-SP-STDBY-4-LIMITS error message appears when rebooting WLSM.

  The following error message may appear when rebooting a WLSM card in a Catalyst 6500 switch:

  ```
  %PM-SP-STDBY-4-LIMITS: The number of VLAN-port instances on module X exceeded the
  recommended limit of 1800
  ```

- CSCsc58565—Clock time zone configured on router is not reflected on WLSM

  For example, if Pacific time is configured on the router (–8 UTC), the WLSM shows UTC time. In addition, if the time zone is configured on the WLSM, it performs and offset on the synchronized time from the router, causing the offsets to be recognized twice.

- CSCee67550—WLSM **show version** output may be confusing to users

  The config-register 0x0 typically indicates that the device is not going to boot completely during the next reload. The WSLM does not allow the configuration register to be modified.

  The statement, "System image file is tftp://255.255.255/unknown" is vague.

  There is no workaround for this problem.

- CSCsb60392—High Supervisor CPU use when the IGMP queue is full causes access point authentication to WDS failures

  When two access points continuously send UDP packets to the Supervisor 720, after a period of time the Supervisor experiences heavy CPU use (approximately 50%), and the following message appears on the console:

  ```
  %MCAST-SP-6-IGMP_PKT_DROPPED: IGMP Queue full (high packet rate/CPU busy), dropped
  1929362 packet(s) in last 5 minutes
  ```

  When this message appears, all access points fail authentication to the WDS.

  This problem is caused by an IGMP version mismatch between the Catalyst 6500 and the 3550 switch. The Supervisor 720 drops and does not process IGMP version 2 packets, but the 3550 switch continues to flood IGMP version 2 packets to the Catalyst 6500, causing the heavy CPU use.

  This problem is can be resolved by one of the following actions:

  - Limit the rate of IGMP packets by applying an IP IGMP snooping rate of 100–600.
  - Apply IP IGMP version 3 to all tunnel or interfaces with mulitcast enabled.

- CSCsc82765—Removing an access point can cause high CPU usage.

  When there are a large number mobile nodes registered on the switch, removing an access point from the system can potentially cause high CPU usage. The problem is a result of traversing the entire list of mobile nodes and deleting those associated to the access point being removed. If the number of mobile nodes is very large the CPU is not relinquished to handle other tasks and can become a CPU hog.

  This problem can occur during normal operation, when the following two conditions are met:

  - A large number of mobile nodes are registered on the switch.
  - An access point removal event occurs due to either crash or disassociation from the WDS.

  **Workaround 1**: Disassociate mobile nodes to reduce the number of mobile nodes registered on the switch before removing the access point.

  **Workaround 2**: Remove WLSMs before removing access points. Doing this starts a graceful recovery process.

# Resolved Caveats in Release 2.1.1

This section describes resolved caveats for the wireless LAN software release 2.1.1:

- CSCsa52581—Spurious memory access and tracebacks no longer occur on one of the active WLSMs in solutions setup
- CSCsc37823—MBSSID with WLSM no longer prevents some devices from obtaining IP addresses.
- CSCsc46670—WLSM now shows CDP information for client access points
- CSCsb56012—Clients can now associate when WDS device is down
- CSCsb60153—The ability of infrastructure access points to learn the IP addresses of passive client devices in a trust mobility network has been improved
- CSCsb89891—DHCP snooping traceback no longer appears in a multiple WLSM HSRP configuration
- CSCsc21683—RPR active Supervisor 720 no longer generates crashinfo file when shutting down
- CSCsc09232—Spurious memory access and traceback no longer occurs on one of the active WLSM's in solutions setup

# Related Documentation

For additional information about Catalyst 6500 series switches and command-line interface (CLI) commands, refer to the following:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720*
- For information about MIBs, refer to this URL:

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

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.