Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Wireless LAN Services Module Software Release 2.3.1

January 18, 2007

This publication describes the features, modifications, and caveats for the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module (WLSM) software release 2.3.1.

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:

Americas 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 2.1.1:

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
	Application Image	Maintenance Image	Application Image	Maintenance Image	
WS-SVC-WLAN-1-K9 with Supervisor Engine 720	1.1.1	3.1(1)	2.2.1	3.1(1)	12.2(18)SXF2

Solution Requirements

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

- Cisco Aironet 1100, 1130AG, 1200, 1230AG, 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
2.3.1	c6svc-wlan-k9w72.3.1.bin	SWSMKW7K9-23
2.2.1	c6svc-wlan-k9w7.2.2.1.bin	SWLSMW7K9-22
2.1.1	c6svc-wlan-k9w7.2.1.1.bin	SWLSMW7K9-21
1.4.1	c6svc-wlan-k9w7.1.4.1.bin	SWLSMW7K9-14
1.3.2	c6svc-wlan-k9w7.1.3.2.bin	SWLSMW7K9-13
1.2.3	c6svc-wlan-k9w7.1.2.3.bin	SWLSMW7K9-12

Features in Software Release 2.3.1

There are no new features in wireless LAN software release 2.3.1.

Features in Software Release 2.2.1

There are no new features in wireless LAN software release 2.2.1.

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 1.4

This section describes the features available in wireless LAN software release 1.4:

- Hardware platforms: Cisco AP1240 series Aironet access point
- Support for Secure Shell (SSH) version 2—SSHv2 is a standards-based protocol that provides secure Telnet capability for router configuration and administration.
- Support for Workgroup Bridge (WGB)—WGBs can associate to a mobility-enabled SSID and provide Layer-3 mobility to WGB wired clients.
- Support for CDP neighbor display for access points (AP)—Wireless Domain Services (WDS) can maintain and display CDP location information of access points.

Features in Software Release 1.3

This section describes the features available in wireless LAN software release 1.3:

- Hardware platforms: BR1310 configured in AP mode
- Local Authentication Server—The WLSM can authenticate up to 50 wireless client devices using LEAP, EAP-FAST, or MAC-based authentication, and perform up to 5 authentications per second.

Features in Software Release 1.2

This section describes the features available in wireless LAN software release 1.2:

- Hardware platforms: Cisco Aironet 1130 series access points
- Support for the VLAN by name feature on the access points

Features in Software Release 1.1

This section describes the features available in wireless LAN software release 1.1:

- Hardware platforms: Cisco Aironet 1100 or 1200 series access points
- Fast, uninterrupted, secure Layer 2 and Layer 3 wireless mobility
- Seamless Layer 3 roaming across subnets
- Radio-management aggregation
- Support for stateful switchover (SSO) with a redundant Supervisor Engine 720
- Wireless domain services (WDS) scalability
  - 300 access points
  - 6000 users
  - 16 different mobility groups (wireless network IDs) per access point
  - Sustained roaming rate of 20 roams per second for wireless LAN clients
  - Burst roaming rate of 100 roams per second for wireless LAN clients

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 2.3.1

These sections describe open and resolved caveats in wireless LAN software release 2.3.1:

- Open Caveats in Release 2.2.1, page 6

Resolved Caveats in Software Release 2.3.1

The following caveats are resolved in wireless LAN software release 2.3.1:

- CSCek46852—EAP-FAST now works with open source clients and local RADIUS sever
- CSCsg91315—WDS now sends appropriate radio scan reports to the WLSE
- CSCsd92405—Router no longer crashes when receiving multiple malfomred TLS and/or SSL3 finished messages
- CSCse85200—Specifically crafted CDP messages no longer cause a router to allocate and keep extra memory
- CSCsb40304—Phone now registers when it is unable to resolve the CCM name
- CSCsf07847—CDP no longer fails to discover neighbor information
- CSCsg70355—Summertime rules are now in accordance with the Energy Policy Act of 2005

Open and Resolved Caveats in Software Release 2.2.1

These sections describe open and resolved caveats in wireless LAN software release 2.2.1:

- Open Caveats in Release 2.2.1, page 6
- Resolved Caveats in Release 2.2.1, page 7

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find select caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Open Caveats in Release 2.2.1

This section describes open caveats for the wireless LAN software release 2.2.1:

- 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.

- 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 2.2.1

This section describes resolved caveats for the wireless LAN software release 2.2.1

- CSCse71792—Message ID Mismatch error no longer occurs in WLSM after failover

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.

- 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

Open and Resolved Caveats in Software Release 1.4.1

These sections describe open and resolved caveats in wireless LAN software release 1.4.1:

Open Caveats in Release 1.4.1

This section describes open caveats for the wireless LAN software release 1.4.1:

- CSCed76695—A computer running Windows 2000 or Windows XP might stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.

  DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch. (CSCef08877)

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.

- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM, or enter the **show mobility stat** command on the supervisor engine.

- CSCef33192—When a client is associating to a mobility-enabled SSID and the client's TCP/IP MTU is greater than 1476 bytes, the client might not be able to download Internet pages, transfer files using FTP, or connect to the Sametime server.

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Enter the **mobility tcp adjust-mss** command on the tunnel interface of the supervisor engine to adjust the TCP MSS value.

  More information about this problem is documented at this URL:

  http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml

Resolved Caveats in Release 1.4.1

This section describes resolved caveats in wireless LAN software release 1.4.1:

- CSCee45312—Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  More details can be found in the security advisory which posted at the following URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050629-aaa

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCeh68178—When a Cisco AP1200 series Aironet access point that is acting as Workgroup Bridge (WGB) associates to a mobility-enabled SSID, the Supervisor Engine 720 might display the following error message:

  ```
  10w3d: %L3MM-4-DUP_IPADDR: MN mac_address is requesting ip ip_address which is being
  used by MN mac_address
  ```

  The IP addresses of the WGB and its wired clients (nodes) might not be correctly programmed in the Layer 3 Mobility Manager (L3MM) database on the Supervisor Engine 720. As a result, traffic to such nodes might be discarded at the Supervisor Engine 720. This problem occurs when there is one or more wired clients attached to the WGB.

This problem is resolved in wireless LAN software release 1.4.1.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCeh54673—Protected access credentials (PAC) auto enrollment fails when a Cisco Compatible Extensions (CCX) client sends both TLS_DH_anon_WITH_AES_128_CBC_SHA (0x0034) and TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033) in the client hello message.

  Workaround: Configure manual PAC provisioning. if the client supports it, or use Access Control Server (ACS) as the RADIUS server.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCei18019—If Layer 3 mobility is enabled on the access point (AP), and mobility trust is enabled on the tunnel interface of the Supervisor Engine 720, then the AP, supervisor engine, and WLSM do not learn the IP addresses of the wireless clients. The output of the **show wlccp ap mobility forwarding** command on the AP does not have an entry for the wireless clients. The output of the **show dot11 association** command shows that the wireless clients are associated. The output of the **show mobility mn** command on the supervisor engine shows that the wireless clients have IP address 0.0.0.0 (under MN IP Address). The output of the **show wlccp wds mobility network-id** command on the WLSM shows "-" as the IP address of the wireless clients. The problem exists in Cisco IOS software Releases 12.3(2)JA2 and 12.3(4)JA.

  Workaround: The problem is temporarily resolved by rebooting the AP.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCsa53672—The command buffer history and cut-and-paste operations do not work properly if you are connected to the WLSM through the console port.

  Workaround: lntroduce a transmit delay for the serial port.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCsa81634—The access point (AP) adds two sets of IP/GRE headers for the packet coming from the mobile node if the AP cannot resolve the IP address of the tunnel endpoint. The first GRE header added is in "fast switch path," the second header is in "process switch path." Typically, these packets are correctly double deencapsulated and forwarded to the correct destination address. However, two sets of IP/GRE headers causes the Supervisor Engine 720 to drop IP packets that are between 1425 bytes and 1448 bytes in length.

  Workaround: Configure static ARP entries on the AP that corresponds to the route processor's mGRE tunnel source addresses by entering the **arp** *ip-address hardware-address* **arpa** *interface* command, for example: **arp 10.10.10.1 00:11:33:44:55:66 arpa bvi1**.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCsa90418—The Wireless LAN Solution Engine (WLSE) might fail to authenticate with the wireless domain services (WDS) that are running Cisco IOS software Release 12.3(4)JA or wireless LAN software release 1.3.1 due to incomplete ARP entries.

  Workaround: Enter the **ip proxy-arp** command to enable proxy ARP on the router that is the first hop from the AP-WDS to the WLSE. If proxy ARP cannot be enabled for some reason, then create a static ARP entry on the AP.

  This problem is resolved in wireless LAN software release 1.4.1.

- CSCeh71021—In wireless LAN software release 1.4.1, the **show wlccp wds ap** command has been enhanced to display CDP neighbor information when used with Cisco Aironet AP running Cisco IOS software Release 12.3(7)JA or later releases:

- **show wlccp wds ap**—added a CDP-NEIGHBOR column
- **show wlccp wds ap mac-address** *mac-address*—added a CDP-NEIGHBOR column and displays the full hostname, IP address, and port ID of the CDP neighbor
- **show wlccp wds ap cdp-neighbor**—introduced to show MAC address, IP address, neighbor name, neighbor IP address, and neighbor port ID information.

Open and Resolved Caveats in Software Release 1.3.2

These sections describe open and resolved caveats in wireless LAN software release 1.3.2:

Open Caveats in Release 1.3.2

This section describes open caveats for the wireless LAN software release 1.3.2:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.
- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.
- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not

release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

- CSCef33192—When a client is associating to a mobility-enabled SSID and the client's TCP/IP MTU is greater than 1476 bytes, the client might not be able to download Internet pages, transfer files using FTP, or connect to the Sametime server.

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Enter the **mobility tcp adjust-mss** command on the tunnel interface of the supervisor engine to adjust the TCP MSS value.

  More information about this problem is documented at this URL:

  http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml)

Resolved Caveats in Release 1.3.2

This section describes resolved caveats in wireless LAN software release 1.3.2:

- CSCei76358—Through normal software maintenance processes, Cisco is removing deprecated functionality from the OS boot routine. These changes have no impact on system operation or feature availability.

Open and Resolved Caveats in Software Release 1.3.1

These sections describe open and resolved caveats in wireless LAN software release 1.3.1:

- Open Caveats in Release 1.3.1, page 15
- Resolved Caveats in Release 1.3.1, page 17

Open Caveats in Release 1.3.1

This section describes open caveats for the wireless LAN software release 1.3.1:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.
- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.
- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

- CSCef33192—When a client is associating to a mobility-enabled SSID and the client's TCP/IP MTU is greater than 1476 bytes, the client might not be able to download Internet pages, transfer files using FTP, or connect to the Sametime server.

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Enter the **mobility tcp adjust-mss** command on the tunnel interface of the supervisor engine to adjust the TCP MSS value.

  More information about this problem is documented at this URL:

  http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml

Resolved Caveats in Release 1.3.1

This section describes resolved caveats in wireless LAN software release 1.3.1:

- CSCef60659, CSCef43691, CSCef44225, CSCsa59600, CSCef44699—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in wireless LAN software release 1.3.1.

- CSCee42617—Users are unable to authenticate using RADIUS, or accounting is not sent to the RADIUS server. In addition, when the **debug radius** command is entered, the following information is generated:

```
RADIUS(00000049): sending
%RADIUS-3-NOSERVERS: No Radius hosts configured.
RADIUS/DECODE: parse response no app start; FAIL
RADIUS/DECODE: parse response; FAIL
```

The output of the **show running-config** command indicates that there are in fact RADIUS servers in the server group.

These issues are observed after following these steps:

a. Remove and recreate a server group that is still referenced by one or more method lists, by entering the following commands:

```
no aaa group server radius XXXX
aaa group sever radius XXXX
server x.x.x.x
...
```

b. Allow one of these method lists to be used, causing a transaction to be sent to a RADIUS or TACACS+ server in the server group.

c. Remove and re-add the **radius-server host ...** command lines for all authentication-capable (or accounting-capable if this group is used for accounting) servers in this server group.

Workaround: Remove all RADIUS or TACACS+ server configurations, remove all RADIUS or TACACS+ server group configurations, and remove all method lists. Then, reconfigure all of them.

This problem is resolved in wireless LAN software release 1.3.1.

- CSCef50742—An 802.1X client may fail to authenticate when the RADIUS State(24) Field values change in between the “Access Challenge” and the “Access Request.”

  This problem is resolved in wireless LAN software release 1.3.1.

- CSCef89795—When you configure Layer 3 mobility on an access point and the access point connects to the WLSM, the access point sends out inter-access point protocol (IAPP) traffic in a non-native VLAN when a wireless client attempts to associate to the access point. There is no loss of functionality.

  This problem is resolved in wireless LAN software release 1.3.1 and Cisco IOS Release 12.3(4)JA on the access point.

- CSCef96534—The WLSM does not properly support TACACS+. Sessions that are configured to authenticate to a TACACS+ server will hang indefinitely.

  Workaround: Use a different method of authentication, such as RADIUS or the local database.

  This problem is resolved in wireless LAN software release 1.3.1.

Open and Resolved Caveats in Software Release 1.2.3

These sections describe open and resolved caveats in wireless LAN software release 1.2.3:

- Open Caveats in Release 1.2.3, page 18
- Resolved Caveats in Release 1.2.3, page 19

Open Caveats in Release 1.2.3

This section describes open caveats for the wireless LAN software release 1.2.3:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.
- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.
- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.
- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.
- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.
- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.
- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

Resolved Caveats in Release 1.2.3

This section describes resolved caveats in wireless LAN software release 1.2.3:

- CSCei76358—Through normal software maintenance processes, Cisco is removing deprecated functionality from the OS boot routine. These changes have no impact on system operation or feature availability.

Open and Resolved Caveats in Software Release 1.2.2

These sections describe open and resolved caveats in wireless LAN software release 1.2.2:

- Open Caveats in Release 1.2.2, page 20
- Resolved Caveats in Release 1.2.2, page 21

Open Caveats in Release 1.2.2

This section describes open caveats for the wireless LAN software release 1.2.2:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.
- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.
- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.
- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.
- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

Resolved Caveats in Release 1.2.2

This section describes resolved caveats in wireless LAN software release 1.2.2:

- CSCef44225—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in wireless LAN software release 1.2.2.

- CSCeg26382—A wireless client is not able to browse the Internet because of an MTU issue caused by the GRE header. To adjust the TCP MSS value of the connection, enter the **mobility tcp adjust-mss** command on the tunnel interface.

  This problem is resolved in wireless LAN software release 1.2.2.

- CSCsa47527—On occasion, when a Protected Extensible Authentication Protocol (PEAP) client performs machine authentication and user authentication through a wireless domain services (WDS) device, the WDS might mistakenly believe that the user authentication that immediately follows the machine authentication is a MAC address spoofing attack. In this situation, the WDS blocks the user from successfully authenticating to the network, but the constant reassociation attempts by the client results in continuous authentication requests being sent to the RADIUS server.

  This problem is resolved in wireless LAN software release 1.2.2.

Open and Resolved Caveats in Software Release 1.2.1

These sections describe open and resolved caveats in wireless LAN software release 1.2.1:

- Open Caveats in Release 1.2.1, page 22
- Resolved Caveats in Release 1.2.1, page 23

Open Caveats in Release 1.2.1

This section describes open caveats for the wireless LAN software release 1.2.1:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.
- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.

- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

Resolved Caveats in Release 1.2.1

This section describes resolved caveats in wireless LAN software release 1.2.1:

- CSCed78149—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

This problem is resolved in wireless LAN software release 1.2.1.

- CSCee38517—The access point does not send an EAP-FAILURE message to a client device that fails authentication when the ACS server sends an ACCESS-REJECT message.

  This problem is resolved in wireless LAN software release 1.2.1.

- CSCef18797—The WDS device now sends the class attribute to participating access points so that the access points can include the attribute in RADIUS accounting messages.

  This problem is resolved in wireless LAN software release 1.2.1; you also need Cisco IOS software Release 12.3(02)JA or later operating on the access points.

Open and Resolved Caveats in Software Release 1.1.2

These sections describe open and resolved caveats in wireless LAN software release 1.1.2:

- Open Caveats in Release 1.1.2, page 24
- Resolved Caveats in Release 1.1.2, page 25

Open Caveats in Release 1.1.2

This section describes open caveats for the wireless LAN software release 1.1.2:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

Workaround: Use an intermediate router to terminate the WAN link, and use a LAN connection between the WAN termination router and the switch.

- CSCee35232—When the Catalyst 6500 system is running in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.
- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.
- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.
- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This condition does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

Resolved Caveats in Release 1.1.2

This section describes resolved caveats in wireless LAN software release 1.1.2:

- CSCed78149—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

This problem is resolved in wireless LAN software release 1.1.2.

- CSCef46191—A specifically crafted Transmission Control Protocol (TCP) connection to a Telnet or reverse Telnet port of a Cisco device running Internetwork Operating System (IOS) may block further Telnet, reverse Telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse Telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet.

  This problem is resolved in wireless LAN software release 1.1.2.

- CSCed78149—TCP connections configured for PMTU discovery might be vulnerable to spoofed ICMP packets. A spoofed ICMP packet might cause the TCP connection to use a very low segment size for 10 minutes at a time.

  This problem is resolved in wireless LAN software release 1.1.2.

- CSCef66214—Uninitialized data fields might be forwarded in WLCCP messages.

  This problem is resolved in wireless LAN software release 1.1.2.

Open and Resolved Caveats in Software Release 1.1.1

These sections describe open and resolved caveats in wireless LAN software release 1.1.1:

- Open Caveats in Release 1.1.1, page 26
- Resolved Caveats in Release 1.1.1, page 28

Open Caveats in Release 1.1.1

This section describes open caveats for the wireless LAN software release 1.1.1:

- CSCed76695—A computer running Windows 2000 or Windows XP may stop responding during initial startup if it uses the default Aironet Client Utilities (ACU) profile that points to a Layer 3 mobility-enabled service set identifier (SSID).

  Workaround 1: Set the MTU on the client network interface to 1476 bytes.

  Workaround 2: Force Windows Kerberos Authentication to use TCP instead of UDP. Microsoft Knowledge Base article 244474 describes this procedure and can be found at this URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;244474

- CSCed16337—A mobile node with a static IP address has IP connectivity in an untrusted network, even though the mobile node should not be able to communicate over an untrusted network. This problem occurs when a mobile node with a static IP address is registered in a trusted network, and then the administrator changes the tunnel interface configuration from trusted to untrusted.

- CSCef08877—DHCP snooping does not work properly if the DHCP packets that are sent to or received from a mobile node are received by the central switch over a WAN link.

  Workaround: Use an intermediate router to terminate the WAN link and use a LAN connection between the WAN termination router and the switch.

- CSCee54884—In a redundant interswitch topology, if you remove the **admin** keyword from the wireless LAN VLAN configuration on the active WLSM, a Layer 3 control protocol (LCP) communication failure occurs between the WLSM and the Layer 3 Mobility Manager on the Supervisor Engine 720. The Supervisor Engine 720 shows the HSRP state as Unknown. However, the HSRP state of the WLSM is still active. As a result, the wireless network is down even though there is a standby WLSM that can service the clients.

  Workaround: Before you modify the wireless LAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module.

- CSCee35232—When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the WLSM from the wireless clients.

- CSCed74302—A mobile node on an untrusted network receives an IP address through DHCP. The DHCP database contains a MAC-to-IP address binding for the mobile node. When the network changes to trusted, the mobile node now has a static IP address. However, if the client does not release the IP address obtained through DHCP, the DHCP database will still contain the MAC-to-IP address binding. If the network returns to untrusted, the mobile node with the static IP address will be incorrectly mapped to the MAC-to-IP address binding in the DHCP database.

  Workaround 1: Release the DHCP-based IP address before assigning a static IP address on the client.

  Workaround 2: Renew the IP address when changing from a static IP address to a DHCP-based IP address on the client.

- CSCee23185—Writing the DHCP database to the bootflash device creates a new file and marks the old file as deleted. However, the old file still exists on the bootflash device. If this process repeats numerous times, read and write processes on the bootflash device become very slow.

  Workaround 1: Enter the **squeeze bootflash:** command to permanently remove all deleted files.

  Workaround 2: Store the DHCP database on an external server.

- CSCee67500—When mobility broadcast is configured on the GRE tunnel interface, the **show wlccp wds mobility** command output does not show the broadcast (B) flag. This does not affect any operation.

  Workaround: Enter the **show wds mn detail** command on the WLSM or enter the **show mobility stat** command on the supervisor engine.

Resolved Caveats in Release 1.1.1

There are no resolved caveats in wireless LAN software release 1.1.1.

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.