Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Wireless LAN Services Module Software Release 1.x

Current Release: 1.4(3)—November 21, 2005
Previous release: 1.4(2), 1.4(1), 1.3(2), 1.3(1) – Deferred, 1.2(3), 1.2(2) – Deferred, 1.2(1), 1.1(2), 1.1(1)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module software release 1.*x*.

Note For installation and configuration procedures for the Wireless LAN Services Module, refer to the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module documentation at this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/wlsm_1_1/index.htm

Contents

This document consists of these sections:

- System Requirements, page 2
- Orderable Software Images, page 3
- Features in Software Release 1.4, page 4
- Features in Software Release 1.3, page 4
- Features in Software Release 1.2, page 4
- Features in Software Release 1.1, page 4
- Limitations and Restrictions, page 5
- Open and Resolved Caveats in Software Release 1.4(3), page 5
- Open and Resolved Caveats in Software Release 1.4(2), page 7
- Open and Resolved Caveats in Software Release 1.4(1), page 8
- Open and Resolved Caveats in Software Release 1.3(2), page 12

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

- Open and Resolved Caveats in Software Release 1.3(1), page 13
- Open and Resolved Caveats in Software Release 1.2(3), page 16
- Open and Resolved Caveats in Software Release 1.2(2), page 18
- Open and Resolved Caveats in Software Release 1.2(1), page 20
- Open and Resolved Caveats in Software Release 1.1(2), page 22
- Open and Resolved Caveats in Software Release 1.1(1), page 25
- Related Documentation, page 26
- Obtaining Documentation, page 26
- Documentation Feedback, page 27
- Cisco Product Security Overview, page 28
- Obtaining Technical Assistance, page 29
- Obtaining Additional Publications and Information, page 30

System Requirements

This section describes the system requirements for the Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module software release 1.x:

- Hardware Requirements, page 2
- Software Requirements, page 3
- Solution Requirements, page 3

Hardware Requirements

The wireless LAN (WLAN) software requires the following hardware:

- Catalyst 6500 series switch or Cisco 7600 series router
- Supervisor Engine 720
- Catalyst 6500 series and Cisco 7600 series Wireless LAN Services Module

Software Requirements

Table 1 lists the WLAN 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
	Application Image	Maintenance Image	Application Image	Maintenance Image		
WS-SVC-WLAN-1-K9 with Supervisor Engine 720	1.1(1)	3.1(1)	2.1.1	3.1(1)	• Cisco IOS Releases 12.2(18)SXD through 12.2(18)SXE5 support all WLSM images, including 1.4(3) and later • Cisco IOS Releases 12.2(18)SXF or later require WLSM images 1.4(3) or later	• Supervisor Engine 720: 12.2(18)SXF • Access points: 12.3(8)JA

Solution Requirements

In addition to the hardware and software requirements, the Wireless LAN Services Module also requires the following:

- Cisco AP1100 or AP1200 series Aironet access points using Cisco IOS Release 12.2(15)XR or Release 12.3(2)JA or later, Cisco AP1130 series Aironet access point using Cisco IOS Release 12.3(2)JA or later, or Cisco Aironet 1310 Outdoor Access Point/Bridge (configured in AP 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 WLAN software.

Table 2 Orderable Software Images

Software Releases	Filename	Orderable Product Number
1.4(3)	c6svc-wlan-k9w7.1.4.3.bin	SWLSMW7K9-14
1.4(2)	c6svc-wlan-k9w7.1.4.2.bin	SWLSMW7K9-14
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 1.4

This section describes the features available in WLAN 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 APs.

Features in Software Release 1.3

This section describes the features available in WLAN software release 1.3:

- Hardware platforms: BR1310 configured in AP mode
- Local Authentication Server—The Wireless LAN Services Module 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 WLAN software release 1.2:

- Hardware platforms: Cisco AP1130 series Aironet access point
- Support for the VLAN by name feature on the access points

Features in Software Release 1.1

This section describes the features available in WLAN software release 1.1:

- Hardware platforms: Cisco AP1100 or AP1200 series Aironet 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 WLAN clients
  - Burst roaming rate of 100 roams per second for WLAN clients

Limitations and Restrictions

This section describes general limitations and restrictions:

- In software release 1.x, you can install one Wireless LAN Services Module in a chassis.
- 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.

Open and Resolved Caveats in Software Release 1.4(3)

These sections describe open and resolved caveats in WLAN software release 1.4(3):

- Open Caveats in Release 1.4(3), page 5
- Resolved Caveats in Release 1.4(3), page 6

Open Caveats in Release 1.4(3)

This section describes open caveats for the WLAN software release 1.4(3):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)
- 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. (CSCed74302)
- 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. (CSCee23185)
- 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 Wireless LAN Services Module, or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)
- 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

  (CSCef33192)

Resolved Caveats in Release 1.4(3)

This section describes resolved caveats in WLAN software release 1.4(3):

- A wireless client remains active on the Wireless LAN Services Module, but the client is not associated to an access point.

  Workaround: Enter the **clear wlccp wds mn mac-address** *mac_addr* command to remove the client entry from the Wireless LAN Services Module. The client can then associate and authenticate properly.

  This problem is resolved in WLAN software release 1.4(3). (CSCsc01606)

Open and Resolved Caveats in Software Release 1.4(2)

These sections describe open and resolved caveats in WLAN software release 1.4(2):

- Open Caveats in Release 1.4(2), page 7
- Resolved Caveats in Release 1.4(2), page 8

Open Caveats in Release 1.4(2)

This section describes open caveats for the WLAN software release 1.4(2):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)

- 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. (CSCed74302)

- 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. (CSCee23185)

- 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 Wireless LAN Services Module, or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

- 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

  (CSCef33192)

Resolved Caveats in Release 1.4(2)

This section describes resolved caveats in WLAN software release 1.4(2):

- 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. (CSCei76358)
- After you configure the **no snmp-server enable traps tty** command and enter the **write mem** command, the **snmp-server enable traps tty** configuration is removed from the startup configuration but remains in the running configuration.

  This problem is resolved in WLAN software release 1.4(2). (CSCee36192)

- After you upgrade to WLAN software release 1.4(1), Secure Shell (SSH) does not function. When you enter the **crypto key generate rsa** command, the console displays the following error message:

  ```
  % Error in generating keys:no available resources
  ```

  This problem is resolved in WLAN software release 1.4(2). (CSCsb66884)

Open and Resolved Caveats in Software Release 1.4(1)

These sections describe open and resolved caveats in WLAN software release 1.4(1):

- Open Caveats in Release 1.4(1), page 9
- Resolved Caveats in Release 1.4(1), page 10

Open Caveats in Release 1.4(1)

This section describes open caveats for the WLAN software release 1.4(1):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)

- 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. (CSCed74302)

- 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. (CSCee23185)

- 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 Wireless LAN Services Module, or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

- 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

  (CSCef33192)

Resolved Caveats in Release 1.4(1)

This section describes resolved caveats in WLAN software release 1.4(1):

- 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://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml

  This problem is resolved in WLAN software release 1.4(1). (CSCee45312)

- 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 WLAN software release 1.4(1). (CSCeh68178)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients.

  This problem is resolved in WLAN software release 1.4(1). (CSCee35232)

- 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 WLAN software release 1.4(1). (CSCeh54673)

- 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 Wireless LAN Services Module 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 Wireless LAN Services Module 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 WLAN software release 1.4(1). (CSCei18019)

- The command buffer history and cut-and-paste operations do not work properly if you are connected to the Wireless LAN Services Module through the console port.

  Workaround: Introduce a transmit delay for the serial port.

  This problem is resolved in WLAN software release 1.4(1). (CSCsa53672)

- 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 WLAN software release 1.4(1). (CSCsa81634)

- 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 WLAN 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 WLAN software release 1.4(1). (CSCsa90418)

- In WLAN 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. (CSCeh71021)

Open and Resolved Caveats in Software Release 1.3(2)

These sections describe open and resolved caveats in WLAN software release 1.3(2):

- Open Caveats in Release 1.3(2), page 12
- Resolved Caveats in Release 1.3(2), page 13

Open Caveats in Release 1.3(2)

This section describes open caveats for the WLAN software release 1.3(2):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)

- 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. (CSCed74302)

- 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. (CSCee23185)

- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

- 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

  (CSCef33192)

Resolved Caveats in Release 1.3(2)

This section describes resolved caveats in WLAN software release 1.3(2):

- 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. (CSCei76358)

Open and Resolved Caveats in Software Release 1.3(1)

These sections describe open and resolved caveats in WLAN software release 1.3(1):

- Open Caveats in Release 1.3(1), page 13
- Resolved Caveats in Release 1.3(1), page 15

Open Caveats in Release 1.3(1)

This section describes open caveats for the WLAN software release 1.3(1):

- 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 (CSCed76695)

- 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. (CSCed16337)
- 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)
- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)
- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)
- 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. (CSCed74302)
- 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. (CSCee23185)
- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

- 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

  (CSCef33192)

Resolved Caveats in Release 1.3(1)

This section describes resolved caveats in WLAN software release 1.3(1):

- 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://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  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 WLAN software release 1.3(1). (CSCef60659, CSCef43691, CSCef44225, CSCsa59600, CSCef44699)

- 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 WLAN software release 1.3(1). (CSCee42617)

- 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 WLAN software release 1.3(1). (CSCef50742)

- When you configure Layer 3 mobility on an access point and the access point connects to the Wireless LAN Services Module, 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 WLAN software release 1.3(1) and Cisco IOS Release 12.3(4)JA on the access point. (CSCef89795)

- The Wireless LAN Services Module 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 WLAN software release 1.3(1). (CSCef96534)

Open and Resolved Caveats in Software Release 1.2(3)

These sections describe open and resolved caveats in WLAN software release 1.2(3):

- Open Caveats in Release 1.2(3), page 17
- Resolved Caveats in Release 1.2(3), page 18

Open Caveats in Release 1.2(3)

This section describes open caveats for the WLAN software release 1.2(3):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)

- 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. (CSCed74302)

- 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. (CSCee23185)

- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

Resolved Caveats in Release 1.2(3)

This section describes resolved caveats in WLAN software release 1.2(3):

- 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. (CSCei76358)

Open and Resolved Caveats in Software Release 1.2(2)

These sections describe open and resolved caveats in WLAN software release 1.2(2):

- Open Caveats in Release 1.2(2), page 18
- Resolved Caveats in Release 1.2(2), page 19

Open Caveats in Release 1.2(2)

This section describes open caveats for the WLAN software release 1.2(2):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)
- 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. (CSCed74302)
- 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. (CSCee23185)
- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

Resolved Caveats in Release 1.2(2)

This section describes resolved caveats in WLAN software release 1.2(2):

- 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://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

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 WLAN software release 1.2(2). (CSCef44225)

- 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 WLAN software release 1.2(2). (CSCeg26382)

- 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 WLAN software release 1.2(2). (CSCsa47527)

Open and Resolved Caveats in Software Release 1.2(1)

These sections describe open and resolved caveats in WLAN software release 1.2(1):

- Open Caveats in Release 1.2(1), page 20
- Resolved Caveats in Release 1.2(1), page 21

Open Caveats in Release 1.2(1)

This section describes open caveats for the WLAN software release 1.2(1):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)
- 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. (CSCed74302)
- 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. (CSCee23185)
- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

Resolved Caveats in Release 1.2(1)

This section describes resolved caveats in WLAN software release 1.2(1):

- 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://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

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 WLAN software release 1.2(1). (CSCed78149)

- 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 WLAN software release 1.2(1). (CSCee38517)

- 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 WLAN software release 1.2(1); you also need Cisco IOS software Release 12.3(02)JA or later operating on the access points. (CSCef18797)

Open and Resolved Caveats in Software Release 1.1(2)

These sections describe open and resolved caveats in WLAN software release 1.1(2):

- Open Caveats in Release 1.1(2), page 22
- Resolved Caveats in Release 1.1(2), page 24

Open Caveats in Release 1.1(2)

This section describes open caveats for the WLAN software release 1.1(2):

- 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 (CSCed76695)

- 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. (CSCed16337)
- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)
- 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)
- When the Catalyst 6500 system is running in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)
- 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. (CSCed74302)
- 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. (CSCee23185)
- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

Resolved Caveats in Release 1.1(2)

This section describes resolved caveats in WLAN software release 1.1(2):

- 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://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  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 WLAN software release 1.1(2). (CSCed78149)

- 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://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in WLAN software release 1.1(2). (CSCef46191)

- 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 WLAN software release 1.1(2). (CSCed78149)

- Uninitialized data fields might be forwarded in WLCCP messages.

  This problem is resolved in WLAN software release 1.1(2). (CSCef66214)

Open and Resolved Caveats in Software Release 1.1(1)

These sections describe open and resolved caveats in WLAN software release 1.1(1):

- Open Caveats in Release 1.1(1), page 25
- Resolved Caveats in Release 1.1(1), page 26

Open Caveats in Release 1.1(1)

This section describes open caveats for the WLAN software release 1.1(1):

- 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 (CSCed76695)

- 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. (CSCed16337)

- 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)

- In a redundant interswitch topology, if you remove the **admin** keyword from the WLAN VLAN configuration on the active Wireless LAN Services Module, a Layer 3 control protocol (LCP) communication failure occurs between the Wireless LAN Services Module 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 Wireless LAN Services Module is still active. As a result, the wireless network is down even though there is a standby Wireless LAN Services Module that can service the clients.

  Workaround: Before you modify the WLAN VLAN IP address or remove the **admin** keyword from the configuration, remove the standby configuration on the active module. (CSCee54884)

- When the Catalyst 6500 system is operating in compact mode, you cannot ping the IP address of the Wireless LAN Services Module from the wireless clients. (CSCee35232)

- 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. (CSCed74302)

- 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. (CSCee23185)

- 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 Wireless LAN Services Module or enter the **show mobility stat** command on the supervisor engine. (CSCee67500)

Resolved Caveats in Release 1.1(1)

There are no resolved caveats in WLAN 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.