Release Notes for Cisco 3200 Series Mobile Access Routers for Cisco IOS Release 12.2(15)JK5

October 11, 2005

These release notes describe new features and significant software components for the Cisco 3200 Series Mobile Access Router that support the Cisco IOS Release 12.2(15)T, up to and including Release 12.2(15)JK5. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.2T* located on Cisco.com.

For a list of the software caveats that apply to Release 12.2(15)JK5, see the "Caveats" section on page 6 and *Caveats for Cisco IOS Release 12.2(15)T*. The online caveats document is updated for every maintenance release and is located on Cisco.com.

Contents

- System Requirements, page 2
- New and Changed Information, page 5
- Limitations and Restrictions, page 6
- Caveats, page 6
- Related Documentation, page 14
- Obtaining Documentation, page 19
- Documentation Feedback, page 20
- Cisco Product Security Overview, page 20
- Obtaining Technical Assistance, page 21
- Obtaining Additional Publications and Information, page 23

CISCO SYSTEMS

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(15)JK5 and includes the following sections:

- Memory Requirements, page 2
- Hardware Supported, page 2
- Determining the Software Version, page 2
- Upgrading to a New Software Release, page 3
- Feature Set Tables, page 3

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by the Cisco IOS Release 12.2(15)JK5 on the Cisco 3200 series routers.

Table 1 Recommended Memory for the Cisco 3200 Series Mobile Access Router

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory	Runs from
Cisco 3201 Wireless Mobile Interface Card	Cisco 3201 WMIC WLAN	Wireless LAN	C3201-k9w7-tar	8 MB	32 MB	RAM

Hardware Supported

The Cisco IOS Release 12.2(15)JK5 supports the Cisco 3201 Wireless Mobile Interface Card (WMIC) card of Cisco 3200 Series Mobile Access Router.

For descriptions of existing hardware features and supported modules, see the configuration guides and additional documents specific to the Cisco 3200 Series Mobile Access Router, which are available on Cisco.com at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Technical Documentation: **Access Servers & Routers**: **Mobile Access Router**

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 3200 series WMIC, log in to the WMIC and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number.

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) 3200 Software (C3201-k9w7-tar), Version 12.2(15)JK5, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.2(15)JA
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* located at http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.2(15)JK supports the same feature sets as Releases 12.2 and 12.2(15)T, but Release 12.2(15)JK includes new features supported by the Cisco 3200 Series Mobile Access Router. Release 12.2(15)JK5 is a rebuild of Release 12.2(15)JK and includes only bug fixes, it does not include any new features.

⚠ **Caution** The Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States will likely require an export license. Customer orders can be denied or subject to delay as a result of United States government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 2 lists the features and feature sets supported in Release 12.2(15)JK5.

The table uses the following conventions:

- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, "12.2(15)JK" indicates that the feature was introduced in 12.2(15)JK. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

Note This feature set table contains only a list of selected features, which are cumulative for Release 12.2(15)nn early deployment releases only (*nn* identifies each early deployment release). The table does not list all features in each image; additional features are listed in *Cross-Platform Release Notes for Cisco IOS Release 12.2(15)T* and in Release 12.2(15)T Cisco IOS documentation.

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router

		Feature Set
Feature	**In**	**Wireless LAN**
Virtual LAN (VLAN)		
802.1q (Trunking, Native Ethernet, 802.1q tagging)	12.2(15)JK	Yes
VLAN Security	12.2(15)JK	Yes
Quality of Service (QoS)		
Priority Voice	12.2(15)JK	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Feature Set
		Wireless LAN
802.1p and 802.1q	12.2(15)JK	Yes
DiffServ Code Point (DSCP)/IP Precedence	12.2(15)JK	Yes
QoS Basic Service Set (QBSS)	12.2(15)JK	Yes
Security		
Wi-Fi Protected Access (WPA)	12.2(15)JK	Yes
Light Extensible Authentication Protocol (LEAP)	12.2(15)JK	Yes
Message Integrity Check (MIC)	12.2(15)JK	Yes
Microsoft Protected Extensible Authentication Protocol (PEAP)	12.2(15)JK	Yes
Fast Secure Roaming		
Wireless Domain Services (WDS) Client Mode	12.2(15)JK	Yes
Cisco Centralized Key Management (CCKM)	12.2(15)JK	Yes
Wireless LAN Context Control Protocol (WLCCP)	12.2(15)JK	Yes
Cisco Key Integrity Protocol (CKIP) + Cisco Message Integrity Check (CMIC)	12.2(15)JK	Yes
Interoperability		
Cisco Aironet 350 Series Bridges	12.2(15)JK	Yes
Cisco Aironet 350 Series Workgroup Bridge (WGB)	12.2(15)JK	Yes
Cisco Aironet 1300 Series Bridge	12.2(15)JK	Yes
Cisco Aironet 1200 Series Access Point	12.2(15)JK	Yes
Cisco Aironet 1100 Series Access Point	12.2(15)JK	Yes
Dynamic Collocated Care-of Address (DCCoA) Dynamic Host Configuration Protocol (DHCP)		
VLAN Roaming with MultiChannel Interface Processor (MIP) in Infrastructure Mode	12.2(15)JK	Yes
DHCP Enhancement	12.2(15)JK	Yes
Miscellaneous		
Transparent Bridging	12.2(15)JK	Yes
Dot11 Radio Driver	12.2(15)JK	Yes
Boot Loader	12.2(15)JK	Yes
Inter-Access Point Protocol (IAPP)	12.2(15)JK	Yes
Rates and Rate Shifting	12.2(15)JK	Yes
Point-to-Point Protocol	12.2(15)JK	Yes
Point-to-Multipoint Protocol	12.2(15)JK	Yes
Packet Concatenation	12.2(15)JK	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

		Feature Set
Feature	**In**	**Wireless LAN**
WGB DHCP	12.2(15)JK	Yes
Hot Standby Access Point	12.2(15)JK	Yes
Publicly Secure Packet Forwarding (PSPF)	12.2(15)JK	Yes
Request To Send/Clear To Send (RTS/CTS) and Fragmentation Thresholds	12.2(15)JK	Yes
Received Signal Strength Indication (RSSI) Measurements	12.2(15)JK	Yes
Simple Network Management Protocol (SNMP) MIB	12.2(15)JK	Yes
Infrastructure Mode		
Root Bridge / Non-Root Bridge	12.2(15)JK	Yes
Root Access Point	12.2(15)JK	Yes
WGB	12.2(15)JK	Yes
Spanning Tree Protocol	12.2(15)JK	Yes

New and Changed Information

The following sections list the new information about the Cisco 3200 Series Mobile Access Router for Release 12.2(15)JK. This information also applies to Cisco IOS Release 12.2(15)JK1, Cisco IOS Relase 12.2(15)JK2, Cisco IOS Release 12.2(15)JK3, Cisco IOS Release 12.2(15)JK4, and Cisco IOS Release 12.2(15)JK5.

New Hardware Features in Release 12.2(15)JK

The following sections describe the new hardware features supported by the Cisco 3200 Series Mobile Access Router for Release 12.2(15)JK.

Cisco 3201 Wireless Mobile Interface Card

The Cisco 3201 Wireless Mobile Interface Card (WMIC) is a mobile interface card (MIC) in a standard PC/104-Plus form factor. It is one component of the Cisco 3200 Series Mobile Access Router and provides an 802.11g wireless interface.

The Cisco 3201 WMIC can be configured as an

- 802.11g wireless access point
- 802.11g wireless root bridge
- 802.11g wireless work group bridge
- 802.11g wireless non-root bridge without clients.

The Cisco 3201 WMIC connects to the Cisco 3200 Series router through the 10/100 Fast Ethernet interface.

The key features of the Cisco 3201 WMIC include the following:

- One autosensing switched 10/100 Fast Ethernet interface.

New Software Features in Release 12.2(15)T

For information regarding the features supported in Cisco IOS Release 12.2(15)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Service & Support: **Technical Documents**: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cross-Platform Release Notes (Cisco IOS Release 12.2(15)T)**

Limitations and Restrictions

The following sections contain limitations that apply to the Cisco 3200 Series Mobile Access Router for Cisco IOS Release 12.2(15)JK. This information also applies to Cisco IOS Release 12.2(15)JK1, Cisco IOS Relase 12.2(15)JK2, Cisco IOS Release 12.2(15)JK3, Cisco IOS Release 12.2(15)JK4, and Cisco IOS Release 12.2(15)JK5.

- CSCed79373—Drop rate is not updated by the **show policy-map interface d0** command.
- CSCee15368—IAPP lost for WGB to Cisco Aironet 1100 access point while configuring LEAP.

Caveats

Caveats describe unexpected behavior or defects in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Release 12.2(15)T are also in Release 12.2(15)JK. For information on caveats in Cisco IOS Release 12.2(15)T, refer to the *Caveats for Cisco IOS Release 12.2(15)T* document. This document lists severity 1 and 2 caveats; the documents is located on Cisco.com.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Release 12.2(15)JK5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

  Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

  Workaround: There is no workaround.

- CSCeb88239

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

  Workaround: There is no workaround.

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

- CSCeg15044

  Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a “No Free TTYs error” message is generated.

  Conditions: This symptom is observed when there are simultaneous Telnet requests.

  Workaround: “clear tcp tcb” should clear the line.

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCsa52807

  A document titled "ICMP Attacks Against TCP," which describes how the Internet Control Message Protocol (ICMP) could be used to perform Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP), has been made publicly available through the Internet Engineering Task Force (IETF) Internet Draft process (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which affect only 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. There are also workarounds available to mitigate the effects. More details can be found in the security advisory at the following URL:

  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

Resolved Caveats - Release 12.2(15)JK4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

Resolved Caveats - Release 12.2(15)JK3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef44225—IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.

  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.

- CSCef44699—GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets

  See note for CSCef44225 above.

- CSCef60659—More stringent checks required for ICMP unreachables.

  See note for CSCef44225 above.

- CSCsa59600—IPSec PMTUD not working [after CSCef44225].

  See note for CSCef44225 above.

Resolved Caveats - Release 12.2(15)JK2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- 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://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.

- CSCee67450

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCef46191—Unable to telnet.

  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

- CSCef84988—Incorrect HTTP Files in TAR.
- CSCin82407

  Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

  Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

  This advisory will be posted to
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

Resolved Caveats - Release 12.2(15)JK1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed73366—The **show tech** command does not show flash output.

  The **show tech** command on Cisco 3201 WMIC does not print the “show flash: all” information.
- CSCed89520—Up to 12 sec needed for ping to pass after roaming.

  When roaming back and forth from one access point to another access point, it sometime takes up to 12 sec for download traffic, for WGB client, to resume. The access point displays that the WGB is associated but traffic does not pass.

  The download traffic is delayed to restart if there is no upload from WGB client after WGB associates to new access point.
- CSCee49654—Wired client of WGB becomes disassociated from Cisco 3201 WMIC (root access point).

  When a WGB and its wired client associate to a Cisco 3201 WMIC configured as a root access point, after approximately 5 min, the wired client is no longer associated, as shown by the **show dot11 associations** command.

  Workaround

  Maintain some traffic going out from the wired client like keepalives or Mobile IP solicitations (if using Mobile IP) continuously being sent at regular time every intervals, where the time interval is less than 5 min. This will ensure the wired client is not timed out on the root access point.

Open Caveats - Release 12.2(15)JK

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee19874—Unexpected exception CPU vector cause WMIC to crash.

  This issue is found by the script only, and happens intermittently. This script performs the following configuration continuously:

  a. Static IP address on BVI1

  b. DHCP address on BVI1

  c. WGB roaming between two bridges

  d. SNMP linkup/down traps send from WGB to MAR

  e. Ping between WGB and bridge.

- CSCee20478—The Cisco 3201 WMIC/Cisco Aironet 1310 bridge console freezes if there is continuous change in Static IP/DHCP.

  When the BVI1 interface is fast configured between static and DHCP IP addresses, sometimes both processes (Exec and DHCP) try to get a semaphore to save the IP address on NVRAM. When one process gets the semaphore, it will still hold the semaphore if it cannot open the file system. At the same time if another process from console tries to get the same semaphore, then the console will be frozen.

  Workaround

  Do not configure the BVI1 interface continuously between static and DHCP IP addresses.

- CSCee35755—WGB 350 does not pass its IP address in Cisco Aironet Ext field in association request.

- CSCee30548—Root bridge cannot ping non-root bridges for point-to-multipoint scenario.

  When VLAN is configured, after the association of a root bridge with two or more non-root bridges, ping from root bridge to non-root bridges fail. The ping will succeed once the non-root bridge entry gets aged and deleted from the root bridge table.

  Workaround

  Disable Spanning Tree Protocol under the VLAN interface.

- CSCee34600—WMIC/Cisco Aironet 1310 bridge advertises SSID when guest mode is disabled.

  The guest-mode SSID is used in beacon frames and probe response frames to probe request that specify the empty or wildcard SSID. If no guest-mode SSID exists, the access point probe response to probe request of empty SSID still contains SSID.

- CSCee44432—When antenna are set to transmit, they will still receive.

  When WMIC antennas are set in transmit or receive mode, they will continue to both transmit and receive.

- CSCee49654—Wired client of WGB becomes disassociated from WMIC (root access point)

  When a WGB and its wired client associate to a WMIC configured as a root Access Point, after approximately 5 min, the wired client is no longer associated as reflected by the **show dot11 associations** command.

  Workaround

  Configure the outgoing traffic from the wired client like keepalives or Mobile IP solicitations (continuously being sent every interval, where the time interval is less than 5 min). This ensures the wired client is not timed out on the root access point.

Resolved Caveats - Release 12.2(15)JK

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)JK and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee33359—WMIC access point reloads when heavy traffic pass through.
- CSCee08584

  Cisco IOS trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for Cisco's IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

  A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml

  Cisco has made free software upgrades available to address this vulnerability for all affected customers.

  This vulnerability is documented by Cisco bug ID CSCee08584.
- CSCed89520—Up to 12 sec needed for ping to pass after roaming.

  When roaming back and forth from one access point to another access point, it sometime takes up to 12 sec for download traffic to resume for WGB client. The access point displays that the WGB is associated but traffic does not pass.

  The download traffic is delayed to restart if there is no upload from WGB client after WGB associates to new access point.

  Workaround

  Configure SNMP link-state trap mechanism between MAR and WMIC.
- CSCed93298—Client does not pass its IP address in the Cisco Aironet Ext field in association request.

  When doing a **show dot11 associations** command on the Cisco 3201 WMIC configured as a root access point, the IP address of any CB21AG client which is associated to the WMIC may be displayed as 0.0.0.0. After two or more minutes, the CB21AG client’s IP address will be displayed correctly.

  Workaround

  Ping the CB21AG client from the Cisco 3201 WMIC, or vice-versa.

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

Related Documentation

The following sections describe the documentation available for the Cisco 3200 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and http://www.cisco.com/univercd/home/index.htm.

Use these release notes with these documents:

- Release-Specific Documents
- Platform-Specific Documents
- Cisco Feature Navigator

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2(15)T*

  On Cisco.com at:

  Products and Solutions: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2**: **Instructions and Guides**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

  Note Cross-Platform Release Notes for Cisco IOS Release 12.2 T are located on Cisco.com or on http://www.cisco.com/univercd/home/index.htm at **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T**.

- Product bulletins, field notices, and other release-specific documents at http://www.cisco.com/univercd/home/index.htm

- *Caveats for Cisco IOS Release 12.2*

  As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T.

  On Cisco.com at:

  Products & Services: **IOS Software**: **Cisco IOS Software Releases 12.2**: **Instructions and Guides**: **Release Notes**: **Release Notes for Cisco IOS Release 12.3, Part 5**: **Caveats**

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

- If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Products and Solutions**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2**: **Troubleshooting**: **Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Documentation specific to the Cisco 3200 Series Mobile Access Router is available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/index.htm

On Cisco.com at:

Products and Solutions: **Routers**: **All Routers**: **Cisco 3200 Series Mobile Access Routers**

On http://www.cisco.com/univercd/home/index.htm at:

Technical Documentation: **Access Servers & Routers**: **Mobile Access Router**

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

Products and Solutions: **Cisco IOS Software**: **Cisco IOS Releases 12.2**: **Instructions and Guides**

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Cisco IOS Release 12.3 Documentation Set Contents

Table 3 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

On Cisco.com at:

Products and Solutions: **Cisco IOS Software**: **Cisco IOS Releases 12.2**: **Instructions and Guides**

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software: **Cisco IOS Release 12.2**

Table 3 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* • *Cisco IOS Configuration Fundamentals and Network Management Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast* • *Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Broadband Access Frame Relay SMDS X.25 and LAPB

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Messages*	

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/univercd/home/home.htm

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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
- Nonemergencies—psirt@cisco.com

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 that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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

- *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

- 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.