Release Notes for Cisco MWR 1941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(15)MC2g

April 19, 2006

Cisco IOS Release 12.2(15)MC2g

OL-13984-16

These release notes are for the Cisco MWR 1941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(15)MC2g. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

For a list of the software caveats that apply to Cisco IOS Release 12.2(15)MC2g, see the "Caveats in Cisco IOS Release 12.2(15)MC2g" section on page 9. To review the release notes for Cisco IOS Release 12.2, go to www.cisco.com and click **Technical Documents**. Select **Release 12.2** from the Cisco IOS Software drop-down menu. Then click **Cisco IOS Release Notes** > **Cisco IOS Release 12.2**.

Contents

This document contains the following sections:

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

Introduction

The Cisco MWR 1941-DC Mobile Wireless Edge Router running Cisco IOS Release 12.2(15) MC2f software is a networking platform optimized for use in mobile wireless networks. It extends IP connectivity to the cell site and Base Transceiver Station (BTS), and through a Fast Ethernet interface to the BTS, provides bandwidth-efficient IP transport of voice and data bearer traffic, as well as maintenance, control, and signalling traffic, over the leased line backhaul network between the BTS and leased line termination and aggregation node via compression (cRTP/cUDP) and packet multiplexing (PPPMux and MLPPP). It supports a limited set of interfaces and protocols, but offers high performance at a low cost while meeting the critical requirements for deployment in cell sites, including small size, extended operating temperature range, high availability, and DC input power flexibility.

System Configuration Requirements

When implemented in a Cisco IP Radio Access Network (IP-RAN) solution, the Cisco MWR 1941-DC router requires the following system configuration:

- Cisco IOS 12.2(8) MC2 or a later Cisco IOS Release 12.2 MC software (excluding Cisco IOS Release 12.2(15)MC1a and Cisco IOS Release 12.2(15)MC2b).
- Network Time Protocol (NTP)

  Network Time Protocol must be configured. The Cisco MWR 1941-DC router uses NTP to maintain a clocking source for the proper time stamping of system messages and log files.
- Redundancy

  When not using the Cisco MWR 1941-DC router in a redundant configuration, the standalone option must be configured from redundancy mode.

  When using the Cisco MWR 1941-DC router in a redundant configuration:
  - Keepalives under the FE must be set to 1.
  - Extended Availability Drop and Insert (EADI) capabilities must be disabled on the router (using the **disable-eadi** global configuration command) to avoid a double-termination situation upon router reboot. If the MWR 1941-DC is not being used in a redundant configuration and EADI is specifically required, you can re-enable EADI using the **no disable-eadi** global configuration command.
  - When attaching the MWR 1941-DC to a device that uses spanning tree, portfast must be configured on the device to avoid problems with HSRP at startup.

- Cisco Express Forwarding (CEF)

  You cannot disable CEF on the MWR 1941-DC. Commands such as **no ip cef** will display an error message "%Cannot disable CEF on this platform." Some commands, such as **no ip route-cache cef**, will not return an error message, however, CEF will not be disabled regardless of whether or not an error message is displayed.

- Hot Standby Router Protocol (HSRP)

  In case of a tie in priority, HSRP uses the IP address to determine the active router. Therefore, you should ensure that the order of the IP addresses of the E1/T1 interfaces of the active router corresponds to the order of the IP addresses of the E1/T1 interfaces of the standby router.

Memory Recommendations

Table 1 Memory Recommendations for the Cisco MWR 1941-DC Mobile Wireless Edge Router

Platform	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWR 1941-DC router	mwr1900-i-mz	32 MB Flash	128 MB DRAM	RAM

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco MWR 1941-DC router, log in to the Cisco MWR 1941-DC and enter the **show version** EXEC command:

```
router> show version
     Cisco Internetwork Operating System Software
     IOS (tm) 1900 Software (MWR1900-I-MZ), Version 12.2(15)MC2a, EARLY DEPLOYMENT RELEASE
     SOFTWARE (fc1)
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to Software Installation and Upgrade Procedures located at the following URL:

http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html

Upgrading to a New ROM Monitor Version

The Cisco MWR 1941-DC router ROM Monitor (ROMMON) consists of two modules:

- A resident module that is not changed during the upgrade procedure.
- An upgradable module that is updated during the upgrade procedure. This is the only module that you will download from Cisco.com.

Note Before performing this procedure, you must download the new ROMMON image from Cisco.com. The download procedure is the same as downloading Cisco IOS software images.

Note In the event of a power outage, the ROM monitor download will not be successful.

Note Command output is similar to the following.

To upgrade the ROMMON version on your Cisco MWR 1941-DC router, complete these steps from EXEC mode:

Step 1 Copy the new ROMMON image from a TFTP server to slot0.

Step 2 Verify that the new image has been copied:

```
Router#dir slot0:
  Directory of slot0:/
  3 -rw- 871 Mar 01 1993 00:05:02 MWR1900-3-default.cfg
  4 -rw- 610704 Mar 01 1993 00:10:30 MWR1900_RM2.srec.122-8r.MC3
```

Step 3 Upgrade the current configuration by entering the **upgrade rom-monitor** command as shown in the following example:

```
Router# upgrade rom-monitor file slot0:MWR1900_RM2.srec.122-8r.MC3
This command will reload the router. Continue? [yes/no]:y
```

Step 4 Press **Enter** to continue. The router begins downloading the ROMMON image. The router automatically reboots.

```
ROMMON image upgrade in progress
Erasing boot flash
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Programming boot flash pppp

Now Reloading
System Bootstrap, Version 12.2(20010915:181836) DEVELOPMENT SOFTWARE
Copyright (c) 1994-2001 by cisco Systems, Inc.

 Running new upgrade for first time

System Bootstrap, Version 12.2(8r)MC3, RELEASE SOFTWARE (fc1)
TAC Support:http://www.cisco.com/tac
Copyright (c) 2002 by cisco Systems, Inc.
mwr1900 processor with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Upgrade ROMMON initialized
rommon 1 >
```

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco MWR 1941-DC router for Cisco IOS Release 12.2(15)MC software.

New Features in the Cisco IOS Release 12.2(15)MC2g

No features are introduced in Cisco IOS Release 12.2(15)MC2g.

New Features in the Cisco IOS Release 12.2(15)MC2f

No features are introduced in Cisco IOS Release 12.2(15)MC2f.

New Features in the Cisco IOS Release 12.2(15)MC2e

No features are introduced in Cisco IOS Release 12.2(15)MC2e.

New Features in the Cisco IOS Release 12.2(15)MC2b

No features are introduced in Cisco IOS Release 12.2(15)MC2b.

New Features in the Cisco IOS Release 12.2(15)MC2a

No features are introduced in Cisco IOS Release 12.2(15)MC2a.

New Features in the Cisco IOS Release 12.2(15)MC2

No features are introduced in Cisco IOS Release 12.2(15)MC2.

New Features in the Cisco IOS Release 12.2(15)MC1

The following features were introduced in Cisco IOS Release 12.2(15)MC1:

- Ignoring the IP ID in RTP/UDP Header Compression, page 6
- Configuring ACFC and PFC Handling During PPP Negotiation, page 6
- Configuring the cUDP Flow Expiration Timeout Duration, page 8

For information on new features in previous Cisco IOS Release 12.2MC software releases, see the platform release notes:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/ipran/1_0/relnotes/index.htm

Ignoring the IP ID in RTP/UDP Header Compression

With Cisco IOS Release 12.2(8)MC2c, IP ID checking was suppressed in RTP/UDP header compression. With Cisco IOS Release 12.2(15)MC1, a new option has been added to the **ip rtp header-compression** interface configuration command that allows you to enable or suppress this checking. The default is to suppress.

To suppress IP ID checking, issue the following command while in interface configuration mode:

Command	Purpose
`Router(config-if)# ip rtp header-compression ignore-id`	Suppresses the IP ID checking in RTP/UDP header compression.

To restore IP ID checking, use the **no** form of this command.

This new feature is identified by CSCdz75957.

Configuring ACFC and PFC Handling During PPP Negotiation

With Cisco IOS 12.2(15)MC1, ACFC and PFC handling during PPP negotiation can be configured.

Configuring ACFC Handling During PPP Negotiation

Use the following commands beginning in global configuration mode to configure ACFC handling during PPP negotiation:

	Command	Purpose
Step 1	`Router(config)# interface` *type slot/port*	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# shutdown`	Shuts down the interface.
Step 3	`Router(config-if)# ppp acfc remote` {**apply** | **reject** | **ignore**}	Configures how the router handles the ACFC option in configuration requests received from a remote peer. • **apply**—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • **reject**—ACFC options are explicitly ignored. • **ignore**—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.

	Command	Purpose
Step 4	`Router(config-if)# ppp acfc local {request | forbid}`	Configures how the router handles ACFC in its outbound configuration requests. • **request**—The ACFC option is included in outbound configuration requests. • **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.
Step 5	`Router(config-if)# no shutdown`	Reenables the interface.

Configuring PFC Handling During PPP Negotiation

Use the following commands beginning in global configuration mode to configure PFC handling during PPP negotiation:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# shutdown`	Shuts down the interface.
Step 3	`Router(config-if)# ppp pfc remote {apply | reject | ignore}`	Configures how the router handles the PFC option in configuration requests received from a remote peer. • **apply**—PFC options are accepted and PFC may be performed on frames sent to the remote peer. • **reject**—PFC options are explicitly ignored. • **ignore**—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.
Step 4	`Router(config-if)# ppp pfc local {request | forbid}`	Configures how the router handles PFC in its outbound configuration requests. • **request**—The PFC option is included in outbound configuration requests. • **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.
Step 5	`Router(config-if)# no shutdown`	Reenables the interface.

To restore the default, use the **no** forms of these commands.

Note For complete details of the ACFC and PFC Handling During PPP Negotiation feature, see the *ACFC and PFC Handling During PPP Negotiation* feature module:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_acf.htm#1025043

Configuring the cUDP Flow Expiration Timeout Duration

To minimize traffic flow corruption, cUDP flows now expire after an expiration timeout duration during which no packets are passed. When this duration of inactivity occurs on a flow at the compressor, the compressor sends a full header upon receiving a packet for that flow, or, if no new packet are received for that flow, makes the CID for the flow available for new use. When a packet is received at the decompressor after the duration of inactivity, the packet is dropped and a context state message is sent to the compressor requesting a flow refresh.

The default expiration timeout is 5 seconds. The recommended value is 8 seconds.

Caution Failure of performance/latency scripts could occur if the expiration timeout duration is not changed to the recommended 8 seconds.

To configure the cUDP flow expiration timeout duration, issue the following command while in multilink interface configuration mode:

Command	Purpose
`Router(config-if)# ppp iphc max-time` *seconds*	Specifies the duration of inactivity, in seconds, that when exceeded causes the cUDP flow to expire. The recommended value is 8.

To restore the default, use the **no** form of this command.

This new feature is identified by CSCeb44623.

Limitations, Restrictions, and Important Notes

Caution The Cisco MWR 1941-DC router does not support online insertion and removal (OIR) of WAN interface cards. Any attempt to perform OIR on a card in a powered up router might cause damage to the card.

Caution Removing the compact flash from the Cisco MWR 1941-DC router during a read/write operation might corrupt the contents of the compact flash, rendering it useless. To recover from an accidental removal of or corruption to the compact flash, a maintenance spare with the appropriate bootable Cisco IOS software image might be needed.

Unsupported Cisco IOS Software Features

The Cisco MWR 1941-DC router requires a special version of Cisco IOS software. Not all Cisco IOS software features can be used with the Cisco MWR 1941-DC router as the core routing is handled by the network processor. The following standard Cisco IOS software features are not supported on the Cisco MWR 1900 router:

- Security Access Control Lists
- MPLS
- 802.1Q VLANs
- Frame Relay (FR)
- MLP LFI
- ATM

Upgrading the VWIC-2MFT-T1-DIR Microcode

When upgrading the image on your Cisco MWR 1941-DC router, power cycle the router or perform a microcode reload on the VWIC-2MFT-T1-DIR to ensure that the firmware for the VWIC-2MFT-T1-DIR is updated during the upgrade.

Disabling PPP Multiplexing

To fully disable PPP multiplexing (PPPMux), issue the **no ppp mux** command on the T1 interfaces of the routers at both ends of the T1 link. If PPP multiplexing remains configured on one side of the link, that side will offer to receive PPP multiplexed packets.

MLP LFI Support

MLP LFI is not supported by the Cisco MWR 1941-DC router. Therefore, MLP LFI must be disabled on peer devices connecting to the Cisco MWR 1941-DC router T1 MLP connections.

ACFC and PFC Support on PPP Interfaces

If upgrading to Cisco IOS Release 12.2(8)MC2c or later for the ACFC and PFC support on PPP interfaces, ensure that you upgrade the MGX-RPM-1FE-CP backcard image first. After doing so, immediately upgrade all MWR 1941-DC routers connected to the MGX-RPM-1FE-CP back card.

Caveats in Cisco IOS Release 12.2(15)MC2g

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC2g. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in 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 Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC2g. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation DVD.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

There are no known open caveats in Cisco IOS Release 12.2(15)MC2g.

Resolved Caveats

This section lists the caveats that are resolved in Cisco Release 12.2(15)MC2g.

- CSCdz37497

  Description: Multicast packets are dropped by IOS until context is re-established.

  This occurs during multicast on one flow at a rate of 100pps or more.

  Workaround: Reduce the PPPMux subframe size on the RPM to a size smaller than a compressed multicast packet so that the multicast packets are not PPPMux'd.

- CSCsd87054 (Duplicate of CSCdz37497)

  Description: An RPM router running Cisco software release122-15.MC2e may drop multicast packets across a multilink interface if the ppp mux is configured on that interface.

  Workaround: Reduce the PPPMux subframe size on the RPM to a size smaller than a compressed multicast packet so that the multicast packets are not PPPMux'd

Caveats in Cisco IOS Release 12.2(15)MC2f

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC2f. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in 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 Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC2f. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T.* These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation DVD.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

This section lists the caveats that are open in Cisco Release 12.2(15)MC2f.

- CSCea73056

  Description: The MWFM or any other NMS system does not get important SNMP traps generated during failover. Up to 50% of the traps are lost.

  During failover the Cisco MWR 1900 router software opens the T1/E1 relays on an active router without taking down the Multilink interface first. The Cisco MWR 1900 routing software keeps sending packets into the disconnected interface for the next few seconds until the interface Multilink goes down. Traps are sent and lost. Traps generated after the link is declared down are kept in the SNMP queue waiting to be routing in order to get restored.

  Workaround: There is currently no workaround.

Resolved Caveats

This section lists the caveats that are resolved in Cisco Release 12.2(15)MC2f.

- CSCsd25168

  Description: The insertion of a GLI card to one of the Fast Ethernet (FE) ports of the Cisco MWR1900 router could cause the Multilink PPP interface to flap leading to a traffic outage for few seconds. A Hot Standby Routing Protocol (HSRP) swap over will also happen.

  The Cisco MWR1900 routers are configured for HSRP redundancy and a GLI card insertion on the active Cisco MWR1900 router would cause the mlppp interface to go DOWN and come UP and would eventually cause the active Cisco MWR1900 router to become standby, and the standby router would then become the active router.

  Workaround: There is no workaround to avoid the Multilink PPP interface from going down. However, to avoid HSRP swap over, the **standby** <*number*> **preempt delay** <*seconds*> commands can be configured. A value of 3 seconds is recommended.

Caveats in Cisco IOS Release 12.2(15)MC2e

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC2e. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in 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 Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC2e. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T.* These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation DVD.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

This section lists the caveats that are open in Cisco Release 12.2(15)MC2e.

- CSCeg37106

  Description: Frame slips were observed on port 0/1 if the T1 cable on port 0/0 was disconnected.

  This situation occurs when the T1 cable connected to the first VWIC port (either port 0/0 or port 0/2) is pulled out from either the MWR side or the FRSM/MPSM side, and frame slips are seen on the remaining port in the same controller.

  Workaround: Connect and disconnect the T1 cable according to following sequence:

  1. Connect port 0/0 first and then port 0/1.

  2. Disconnect port 0/1 first and then port 0/0

  3. Perform the same procedure to ports 0/2 and 0/3.

Resolved Caveats

This section lists the caveats that are resolved in Release 12.2(15)MC2e.

- CSCea73056

  Description: Mobile Wireless Fault Mediator (MWFM) or any other Network Management System (NMS) does not receive important Simple Network Management Protocol (SNMP) traps generated during failover. Up to 50% of the traps are lost.

  During failover, the MWR 1900 routing software opens T1/E1 relays on the active router without taking down the Multilink interface first. The MWR 1900 routing software keeps sending packets into the disconnected interface for the next few seconds until the Multilink interface goes down. Traps are sent and lost. Traps generated after the link is declared down are kept in the SNMP queue waiting for the routing to become restored.

  Workaround: There is currently no workaround.

- CSCec20844

  Description: If a virtual access interface is created and that interface is assigned to a multilink group interface by the application of the **ppp multilink group** *group-number* interface configuration command, then when the interface goes down, the configuration is not properly removed when the virtual access interface is recycled for reuse.

  Perhaps the most visible effect of this symptom, is that if the virtual access interface negotiates to use multilink during a future session (a different use of the virtual access interface than the one when the interface was first created), the interface does not join the designated multilink group interface. Instead, a separate virtual access interface is created for the bundle. This behavior may lead to additional problems since the multilink bundle interface that is created probably does not have the desired configuration that is required for the connection.

  This symptom is observed on all Cisco platforms that are running Cisco IOS Release 12.2(5) and later.

  Workaround: There is currently no workaround.

- CSCec46798

  Description: A router may reload with a bus error when the Point-to-Point protocol (PPP) sessions are disconnected.

This symptom is observed on a Cisco router that is running an interim release of Cisco IOS Release 12.3(4). The symptom occurs on PPP sessions that are not directly associated with an interface or a subinterface (for example, PPP over ATM [PPPoATM] or Layer 2 Tunneling Protocol [L2TP]). Earlier releases of Cisco IOS software do not display this symptom.

Workaround: There is currently no workaround.

- CSCec58486

  Description: A Cisco 7200 router may unexpectedly reload. This problem occurs when the router attempts to correct a single bit error in memory (DRAM parity). The symptoms are similar to CSCdu00306 however CSCdu00306 may not correct every situation where this may occur.

  This symptom is specific to Network Processing Engine (NPE-400).

  Workaround: There is currently no workaround.

- CSCed27956 (duplicate of CSCed38527)

  Description: A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or Secure Shell [SSH] session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

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

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml

  It describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml

- CSCed40933

  Description: 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 (triplicate of CSCef6059 and CSCef61610)

  Description: 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:

a. Attacks that use ICMP “hard” error messages.

b. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.

c. 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.

More details can be found in the security advisory which 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.

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

http://www.cpni.gov.uk/Products/advisories.aspx

- CSCef36231

  Description: A Hot Standby Routing Protocol (HSRP) tracking configuration is not accepted when you re-enter the configuration after you first delete it.

  This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or Release 12.3T.

  Workaround: Configure interface tracking by entering the **track 100 interface e2/3 line-protocol** command. Then, set the HSRP group to track the tracking object number by entering the **standby 1 track 100** command.

- CSCef46191

  Description: 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.

  User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

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

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

- CSCef67682

  Description: Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
    ipv6 traffic-filter nofragments in
```

```
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at

http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- CSCef68324

  Description: Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack 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 which is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

- CSCeg60667

  Description: In an active router, the relays are closed and the revertive interface should be in the ADMINDOWN state. However, when the interface is brought up, the command **standby use-interface loopback 102 revertive** is re-issued. This is causing an issue with Hot Standby Routing Protocol (HSRP) as the difference of HSRP priorities between the active and standby routers is no longer 5 but 10. As a result, a router swap will not occur when a single interface goes down.

  This situation occurs when re-configuring the redundancy command which brings up **revertive int lo102**.

  Workaround: Manually shut the interface down if it is re-configured.

- CSCeg76600

  Description: When the **no shutdown** command is configured on a Multilink interface, some links that are members of the multilink bundle may fail to renegotiate the PPP Link Control Protocol (LCP) and thus fail to activate the bundle.

  This symptom occurs very rarely, and is usually associated with several multilink member links and the use of the **shutdown** and **no shutdown** commands in rapid succession on the Multilink interface.

  Workaround: Configure **shutdown** on the Multilink interface, wait a few moments, then configure **no shutdown**.

- CSCeh13489

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

  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 a 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 the event is recorded in the log.

- CSCeh33220

  Description: When an FE cable is pulled out of a Cisco MWR 1900 Mobile Wireless Edge Router, a LINK DOWN Trap is generated. When the cable is inserted back in, the LINK DOWN Trap is generated again, instead of the LINK UP Trap.

  This symptom occurs when the FE cable is pulled out and re-inserted in the Cisco MWR 1900 Mobile Wireless Edge Router.

  Workaround: There is currently no workaround.

- CSCeh54591

  Description: The MWR controllers are down when the ‘detect v54 channel-group’ is configured.

  This symptom occurs when you Boot both redundancy MWRs at the same time. Some of the controllers can go down in the active MWR.

  Workaround: Reload the active MWR to cause a failover. All the controllers will come up after the standby router becomes the active router.

- CSCei61732

  Description: 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

- CSCei76358

  Description: 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.

- CSCei77821

  Description: Array indexing on toaster address queue may go out of array boundary. This may cause a crash or exhibit unexpected behavior.

  Workaround: There is currently no workaround.

- CSCsb17120

  Description: When you send traffic through a link, after a few seconds the packets of traffic that are sent through the link are not incrementing, even though the Chars Out display clearly shows the packets are incrementing.

  Workaround: There is currently no workaround.

Caveats in Cisco IOS Release 12.2(15)MC2b

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC2b. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in 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 Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC2b. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation DVD.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

There are no known open caveats in Cisco IOS Release 12.2(15)MC2b.

Resolved Caveats

This section lists the caveats that are resolved in Release 12.2(15)MC2b.

- CSCeb86268

  Description: An adjacent T1 link keeps having CRC input errors if the peer router has its T1 link shut. The serial interface on the router in question would keep resetting.

  This problem only occurs on the GT96K serial interface when the peer router has its adjacent T1 link shut. This problem is observed in Cisco IOS 12.2T and 12.3.

  Workaround: Shut down the T1 link on the router in question.

- CSCec86420

  Description: Cisco routers running Cisco IOS supporting Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attacks on the MPLS disabled interfaces.

  This vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  This bug is a complementary fix to CSCeb56909 which addresses this vulnerability.

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

  http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml

- CSCee75683

  Description: When a standby router is reloaded, it takes over as the active router.

  This occurs more often when the IP address of the standby router is higher than the active router. Pre-emption occurs on reload.

  Workaround: Unconfigure pre-emption when reloading the standby router if this additional swap over is considered an inconvenience and the outage is not considered acceptable.

- CSCsa81379

  Description: NetFlow Feature Acceleration CLI.

NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

This removal does not require an upgrade of your existing installation.

The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

cnfFeatureAcceleration	1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable	1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot	1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot	1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable	1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry	1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType	1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot	1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive	1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges	1.3.6.1.4.1.9.9.99999.1.3.4.1.6

Caveats in Cisco IOS Release 12.2(15)MC2a

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC2a. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in 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 Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC2a. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation DVD.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

The caveats listed in this section are open in Cisco IOS Release 12.2(15)MC2a.

- CSCdz37497

  Description: When PPPMux and cUDP are configured, during periods of sustained multicast traffic at a rate of 100 pps or more causes a periodic “out-of-sequence” condition in the MWR 1941-DC IOS decompression.

  Workaround: Reduce the rate of multicast traffic.

- CSCea73056

  Description: During a failover, the MWR 1941-DC router software opens T1/E1 relays on the active router without taking down the multilink interface first. Packets are sent to the disconnected interface for the next several second until the multilink interface is declared down. This condition causes the network management system to not receive SNMP traps generated during the failover.

  Workaround: There is currently no workaround.

- CSCea85262

  Description: When shutting down a multilink interface, the virtual access (VA) interface associated with the multilink interface flaps.

  Workaround: Shut down the subinterface associated with the multilink group.

Resolved Caveats

This section lists the caveats that are resolved in Release 12.2(15)MC2a.

- CSCdz32659

  Description: Memory allocation failure (MALLOCFAIL) messages no longer occur for Cisco Discovery Protocol (CDP) processes.

- 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.

- CSCec25430

  Description: A Cisco device reloads on receipt of a corrupt CDP packet.

- CSCec55704

  Description: The carrier delay detects interface flaps and closes a serial interface even though the carrier delay timer was not exceeded.

- CSCec85345

  Description: On occasion, when an MWR 1941-DC router relay closes, syslog messages report the relay as opening.

- CSCed23981

  Description: When a PPP multiplexed ICMP echo request is sent to an MWR 1900 series router, the MWR 1941-DC router corrupts the ICMP data payload when de-multiplexing the ICMP packets.

- CSCed40563

  Description: Problems with the CDP protocol have been resolved.

- CSCin67568

  Description: A Cisco device experiences a memory leak in the CDP process. The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Unreproducible Caveat

The caveat listed in this section has not been reproduced during testing. In the unlikely event you experience the problem described in this section, contact Cisco customer service.

- CSCdz48133

  Description: Periods of sustained mixed traffic (UDP multicast, IP, and TCP) might cause the MWR 1941-DC router to crash.

Troubleshooting

Collecting Data for Router Issues

To collect data for reporting router issues, issue the following command:

- **show tech-support**—Displays general information about the router when it reports a problem.

Collecting Data for Redundancy Issues

To collect data for redundancy-related issues, issue the following commands while in EXEC mode:

- **show cdp neighbors**—Displays detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP).
- **show controllers**—Displays information that is specific to the hardware.
- **show ip interface**—Displays the usability status of interfaces configured for IP.
- **show redundancy**—Displays current or historical status and related information on redundant Dial Shelf Controllers (DSCs).
- **show standby**—Displays Hot Standby Router Protocol (HSRP) information.
- **show standby brief**—Displays Hot Standby Router Protocol (HSRP) information; specifically, with the brief keyword specified, a single line of output summarizing each standby group.

Collecting Data for ROMmon Issues

To collect data for ROMmon issues, issue the following command while in EXEC mode:

- **showmon**— Displays currently selected ROM monitor.

Collecting Data for Router Rebooting to ROMmon

If a router reboot to ROMmon occurs, issue the **dir** *device ID* command where *device ID* is slot0:, and look for the router processor or network processor exception file (crashinfo* or pxf_crashinfo* respectively). Once you have located one of these files, you can email the file along with a description of the problem to your Cisco representative.

Documentation Updates

The following sections describe updates to the published documentation for the Cisco MWR 1941-DC router. The heading in this section corresponds with the applicable section title in the documentation.

Configuring RTP/UDP Compression

The maximum number of RTP header compression connections per MLP bundle is documented as 600 when in fact, up to 1000 connections are supported on an interface. This change also applies to the **ip rtp header-compression** command description.

The show ip rtp header-compression Command

The **detail** keyword is not supported in the **show ip rtp header-compression** command. Therefore, output does not display for the `detail` keyword if it is specified in command.

Configuring T1 Interfaces

Some configuration modes shown in the procedure for configuring T1 interfaces in the "Configuring T1 Interfaces" of the *Cisco MWR 1900 Software Configuration Guide* are incorrect. The correct command modes are as follows:

Step 1 Specify the controller that you want to configure. For information about interface numbering, see the *Understanding Interface Numbering* section.

```
Router(config)# controller t1 slot/port
```

Step 2 Specify the framing type.

```
Router(config-controller)# framing esf
```

Step 3 Specify the line code format.

```
Router(config-controller)# linecode b8zs
```

Step 4 Specify the channel group and time slots to be mapped. For the VWIC interfaces, you can configure two channel-groups (0 and 1) on the first T1 port or you can configure one channel-group (0 or 1) on each T1 port. Once you configure a channel group, the serial interface is automatically created.

Note The default speed of the channel group is 56. To get full DS0/DS1 bandwidth, you must configure a speed of 64.

```
Router(config-controller)# channel-group 0 timeslots 1-24 speed 64
```

Step 5 Configure the cable length.

```
Router(config-controller)# cablelength feet
```

Note Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Step 6 Exit controller configuration mode.

```
Router(config-controller)# exit
```

Step 7 Configure the serial interface. Specify the T1 slot (always 0), port number, and channel group.

```
Router(config)# interface serial slot/port:0
```

Step 8 Assign an IP address and subnet mask to the interface. If the interface is a member of a Multilink bundle (MLPPP), then skip this step.

```
Router(config-if)# ip address ip_address subnet_mask
```

Step 9 Before you can enable RTP header compression, you must have configured a serial line that uses PPP encapsulation. Enter the following command to configure PPP encapsulation.

```
Router(config-if)# encapsulation ppp
```

Step 10 Set the carrier delay for the serial interface.

```
Router(config-if)# carrier-delay number
```

Step 11 Return to Step 1 to configure the second port on the VWIC and the ports on any additional VWICs.

Step 12 Exit to global configuration mode.

```
Router(config-if)# exit
```

Configuring Redundancy

Before configuring redundant MWR 1941-DC routers as described in the “Configuring T1 Interfaces” section of the *Cisco MWR 1900 Software Configuration Guide*, ensure that you disable EADI capabilities on the router by issuing the **disable-eadi** global configuration command as follows:

```
Router(config)# disable-eadi
```

Related Documentation

The following sections describe the documentation available for the Cisco MWR 1941-DC router. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Platform-Specific Documents

These documents are available for the Cisco MWR 1941-DC router on Cisco.com and the Documentation CD-ROM:

- Cisco MWR 1941-DC Mobile Wireless Edge Router
  - *Cisco MWR 1941-DC Hardware Installation Guide*
  - *Cisco MWR 1900 Software Configuration Guide*
  - *Cisco MWR 1941-DC Rack Mounting Instructions*
  - *Cisco MWR 1941-DC Regulatory Compliance and Safety Information*
- *VWIC-2MFT-T1-DIR, VWIC-2MFT-E1-DIR Installation Instructions*
- *MGX-RPM-1FE-CP Back Card Installation and Configuration Note*

On Cisco.com at:

Technical Support and Documentation: Routers: Cisco MWR 1900 Mobile Wireless Routers:

On the Documentation DVD at:

Routers: Cisco MWR 1900 Mobile Wireless Routers:

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2 MC and are updates to the Cisco IOS documentation set. A feature module consists of an overview of the feature, configuration tasks, and a command reference.

On Cisco.com at:

Technical Documentation: Cisco IOS Software: Cisco IOS Release 12.2: New Feature Documentation:12.2-Based New Features: New Features in Release 12.2 MC

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.htm

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

Release Notes for Cisco MWR 1941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(15)MC2g