Doc. No. 78-3753-01

Channel Interface Processor (CIP) Microcode Release Note and Microcode Upgrade Requirements

Product Numbers: All software bundles for Cisco IOS Release 11.2(1) and later.

Starting with Cisco Internetwork Operating System (Cisco IOS™) Release 11.1 and continuing with Cisco IOS 11.2, microcode images for the Channel Interface Processor (CIP) are bundled separately from the Cisco IOS software. This document describes specific CIP microcode issues up to and including Release 11.2(1).

Caution If you are upgrading from a previous Cisco IOS release, a special microcode installation procedure is required or your CIP will not operate properly. For details, refer to the section "CIP Microcode Upgrade Overview" on page 7.

Introduction

This CIP microcode release note describes the CIP microcode modifications and caveats for the latest version of CIP microcode. It includes all CIP microcode releases used in conjunction with Cisco IOS Release 11.2. Also included is an overview of the procedures required to upgrade to the latest versions of CIP microcode depending on the CIP-compatible router platform you have.

This CIP microcode release note discusses the following topics:

- Cisco Connection Online, page 8
- Cisco Connection Documentation, page 10

Cisco IOS Software and Cisco 7000 Family Hardware Documentation

For documentation of CIP features in Cisco IOS Release 11.2, refer to the following Cisco IOS Release 11.2 publications (customer order numbers included):

- *Configuration Fundamentals Configuration Guide* (DOC-CFCG11.2=)
- *Configuration Fundamentals Command Reference* (DOC-CFCR11.2=
- *Bridging and IBM Networking Configuration Guide* (DOC-IBMNCG11.2=)
- *Bridging and IBM Networking Command Reference* (DOC-IBMNCR11.2=)
- *Cisco IOS Software Command Summary* (DOC-CIOSCS11.2=)
- *System Error Messages* (DOC-SYSEM11.2=)
- *Release Notes for Cisco IOS Release 11.2* (Document Number 78-3648-01-xx)

These publications are available on Cisco Connection Online in the Cisco IOS 11.2 database.

For chassis-specific hardware configuration or troubleshooting information, refer to the following publications:

- *Cisco 7000 Hardware Installation and Maintenance* (DOC-7000IM3)
- *Cisco 7010 Hardware Installation and Maintenance* (DOC-707IM2)
- *Cisco 7505 Hardware Installation and Maintenance* (DOC-7505HIM1)
- *Cisco 7507 Hardware Installation and Maintenance* (DOC-7507HIM1)
- *Cisco 7513 Hardware Installation and Maintenance* (DOC-7513HIM1)

These hardware publications are available on Cisco Connection Online in the Core/High-End Routers database.

How Does CIP Microcode Ship?

For the Cisco 7000 family routers (Cisco 7000 series and Cisco 7500 series), CIP microcode is available on floppy disks, Flash memory cards (which also include the Cisco IOS release compatible with the microcode version), and via Cisco Connection Online (CCO).

Starting with Cisco IOS Release 11.1 and continuing with Cisco IOS Release 11.2, CIP microcode images are shipped separately from the Cisco IOS software. For new Cisco 7000 family routers shipped with Cisco IOS Release 11.2, the CIP microcode is shipped pre-installed on the Flash memory card. For Cisco IOS Release 11.2 software upgrades, the CIP microcode is shipped or available on the following media:

- Via electronic download from Cisco Connection Online (CCO) using File Transfer Protocol (FTP) for all Cisco 7000 family routers
- On a separate set of floppy disks shipped with Cisco IOS Release 11.2 disks for all Cisco 7000 family routers
- On floppy disks shipped with Cisco IOS Release 11.2 ROMs (RP-based Cisco 7000 series routers only)

- Pre-installed on a Flash memory card with Cisco IOS Release 11.2 (available as an upgrade for RP-based Cisco 7000 series routers only)

CIP Microcode and CIP Hardware Compatibility

Production of the initial CIP card has been discontinued and it can no longer be ordered. The CIP2 card replaces the CIP.

There are no microcode issues associated with this change. The Route Switch Processor (RSP) card in the Cisco 7000 family router automatically determines which version of the microcode is appropriate for the installed CIP or CIP2.

Cisco IOS Release 11.2(1) and CIP microcode Version 22.7 support both a CIP and a CIP2 card in the same router.

CIP Microcode/Cisco IOS Software Compatibility Matrix

Table 1 lists CIP microcode version and Cisco IOS software compatibility for the Cisco 7000 family. The CIP microcode image is shipped in a separate bundle from the Cisco IOS software images.

Note Starting with Cisco IOS Releases 10.3(9) and 11.0(5) and continuing with Cisco IOS Release 11.2(1), the 7000 series routers and the 7500 series routers use the same CIP microcode image. The first version of common CIP microcode in Cisco IOS Release 10.3 is cip20-5, in Cisco IOS Release 11.0 it is cip21-3. Cisco IOS Release 11.1 and later all use the common CIP microcode.

Table 1 Cisco IOS Releases and CIP Microcode Releases for the Cisco 7000 Family

Cisco IOS Release	Default CIP Microcode Version	Minimum CIP Microcode Version Required
11.1(1)	22.7 (slot0:cip22-0)	22.0
11.1(2)	22.0 (slot0:cip22-0)	22.0
11.1(3)	22.0 (slot0:cip22-3)	22.3
11.1(4)	22.0 (slot0:cip22-3)	22.3
11.1(5)	22.0 (slot0:cip22-6)	22.6
11.1(6)	22.0 (slot0:cip22-7)	22.7
11.2(1)	22.0 (slot0:cip22-10)	22.10

CIP Microcode Caveats and Modifications

The following sections describe the caveats to current CIP microcode versions and the modifications made in current CIP microcode versions. The caveats listed apply to only the most serious problems.

Caveats for Version 22.7/Version 22.10 Modifications

This section describes possibly unexpected behavior by Version 22.7. All the caveats listed in this section are resolved in Version 22.10.

- Historically both the default and maximum values for the tn3270 server “maximum-lus” parameter were set at 20000. Due to licencing issues, the default value will be set to 2100; the maximum value will become 32000. Licence reminders will be displayed when the default is exceeded, and warning messages displayed when the configured maximum is approached. [CSCdi62250]
- Under some circumstances, static TN3270 LUs cannot be selected by name by the client. The LU is active at the Host and at the CIP but attempts to select it are refused as though it were unknown.

  The more static LUs, the higher the chance that any given one is affected. [CSCdi67583]
- For CIP CSNA users who is running IOS version 11.0(11) you should download one or both of the following microcode images from CCO.

  cip21-10 for CIP 1

  cipp21-10 for CIP 2

  There is a potentially catestrophic problem with the CSNA feature in the microcode bundled with IOS verion 11.0(11). The problem can occur with SNA PIUs 4025 bytes or greater destined for the channel. [CSCdi69773]

Caveats for Version 22.3/Version 22.6 Modifications

This section describes possibly unexpected behavior by Version 22.3. All the caveats listed in this section are resolved in Version 22.5. There was no released microcode Version 22.4 or 22.5.

- This fix address a CSNA problem. While in the process of bringing up a session or in data transfer phases, VTAM deactivates all active sessions with following error message: INOP RECEIVED FOR XXXXXXXX code = 02 [CSCdi64229]
- The CIP was designed to run two channel adapters with only 2MB of DRAM when running IP Datagram mode. When customers ran 32 CLAW devices with RIP, packets would be dropped even though additional DRAM was available to buffer packets until the mainframe could receive them. This change allows CIPs with more than 2MB of DRAM to make use of the additional memory when running IP Datagram mode. [CSCdi54042]
- This fix addresses unexpected behavior when running CSNA, which could potentially cause session failure, BADFIFO error messages, and other side effects. [CSCdi61131]
- Under certain conditions the File Transfer Protocol (FTP) server on VM or MVS stops functioning if the offload device returns an invalid return code to a particular socket request to receive data. This return code also generates a traceback in the TCPIP logs for TCPIP for VM and MVS. The offload device no longer returns this invalid return code. [CSCdi61870]

Caveats for Version 22.0/Version 22.3 Modifications

This section describes possibly unexpected behavior by Version 22.0. All the caveats listed in this section are resolved in Version 22.3.

- Hub terminals manufactured by HOB expect a Receive Ready (RR) to be sent after the SABME is sent. This is not required by the 802.2 standard. After the HOB sends a SABME to the CIP LLC stack, the CIP LLC stack should respond with an RR and then assume that the terminal is in normal transfer mode. [CSCdi45083]

- The Offload read and write tasks are created with too little stack space. Under certain conditions, typically when several hundred sessions are established, a stack overflow can occur, which usually leads to a fatal error dump. The error code in this dump can be almost anything, with 32 and 35 being most likely. If you are running Offload with microcode versions cip21-3, cip11-4, cip22-1, or earlier, you should upgrade to at least cip21-4 (Cisco IOS Release 11.0(7) or later) or cip22-3 (Cisco IOS Release 11.1(2.4) or later). [CSCdi48357]
- When running CSNA, during large bursts of LLC, type 1 traffic from VTAM (many sessions configured for callout) an automatic reload of the CIP microcode may occur with the following message displayed: SSI_ASSERT failure in../cta/cta_mbuf.c @ 287 ... [CSCdi48855]
- When running MVS V=R in a VM/XA guest machine with a PCA, the mainframe channel will generate an interface disconnect in the middle of command chaining when it reaches an invalid CCW. If multiple devices are active on the PCA, this may result in an SCB_CHAIN error. The only work around for the SCB_CHAIN error is not to run in this configuration. [CSCdi49057]
- When running CSNA, if XCA major nodes are cycled inactive/active many times without reloading the CIP microcode, a CCA error message TOOMANY may be seen, and channel operation is paused without completing the current channel program. Depending on traffic levels, operation may or may not resume. If not, the CIP microcode must be reloaded. [CSCdi51452]
- Restarting TCPIP on the mainframe while data is moving through an Offload connection can cause the CIP to halt unexpectedly. The result is a fatal error dump. This dump must be sent to development engineering for analysis. The problem can be avoided by shutting down TCPIP, which causes all open sockets/connections to be closed, before restarting it. [CSCdi51859]
- With the CSNA feature, if an XCA major node is inactivated or VTAM is shut down while connections are active and traffic is flowing to VTAM, the CIP may pause indefinitely. If this pause occurs, the CIP microcode must be reloaded. [CSCdi53138]

Caveats for Version 21.3/Version 22.0 Modifications

CIP Microcode Version 22.0 was the first version specifically built for unbundled microcode support under Cisco IOS Release 11.1. Because CIP Microcode Version 22.0 was based on Version 21.3, modifications made in Version 21.3 are listed below.

Modifications

CIP Microcode Version 21.3 fixed the following:

- This fix handles the VTAM flow request and eliminates the following message from being displayed: CSNA code does not recognize 0x0d50, Flow Request from VTAM [CSCdi45035]
- If the host sends a CLAW disconnect message to a link that has already been disconnected and that CLAW connection has a different link that is connected, the CIP will cause the static route for the CLAW connection to be removed. Older version of Interlink (2.1) and IBM TCPIP V2 behave in this manner.

  The router will show that the Claw connection, as viewed by **show extended channel** *slot/port* **statistics** is connected, but the static route will be removed. [CSCdi45752]
- When status is pending on initial connection, the pending status is not flushed. This resulted in owed status being suppressed. On CSNA connections this causes data transfer to stop, and VTAM or the Missing Interrupt Handler detects an operation as taking too long. [CSCdi46037]
- This fix only applies to CSNA users who are using host backup configuration. If the user has duplicate VTAMs, for backup purposes, the user can configure two or more logical LAN adaptors (ADAPNO) with same MAC address on different internal LANs. When one of the

VTAMs is brought down, similar to varying off the XCA major node, or one of the VTAMs is in trouble, all end-stations that previously connected to the problem VTAM can then reconnect to the backup VTAM.

The subroutine that handles the reconnect logic requires this fix. [CSCdi47267]

CIP-Related Caveats for Cisco IOS Release 11.2(1)

For a complete list of caveats against Cisco IOS Release 11.2(1), use Cisco Connection Documentation or access Cisco Connection Online as described in the section "Cisco Connection Online" later in this document. You can also refer to the *Release Notes for Cisco IOS Release 11.2* publication (Document Number 78-2886-xx), which is available on Cisco Connection Documentation.

CIP and Processor Module ROM Monitor Recommendations

CIP and processor module (RP, RSP, and RSP7000) ROM monitor (system bootstrap) versions and system software images are typically independent of each other; however, the CIP hardware version does have minimum recommended requirements in terms of Cisco IOS Release and CIP Microcode Version as listed in Table 2. Other microcode versions can be used, but only when specifically instructed to do so by technical support personnel. Table 3 identifies the processor module monitor versions.

Use the **show diag** exec command to display the CIP hardware version. The original CIP card is identified as version 4.x. The CIP2 card is identified as version 5.x.

Table 2 CIP Hardware, Cisco IOS, and CIP Microcode Compatibility

CIP Hardware Version	Minimum Cisco IOS Release Required	Minimum CIP Microcode Version Recommended
CIP 4.1	10.2(4.6)	cip10-4
CIP 4.2	10.3(5.1)	cip10-7
	10.3(8.5)	cip20-5
	10.3(6.2)	rsp_cip20-2
CIP 4.4[1]	10.2(10.2) or later	cip10-4
		cip20-4
	10.3(7.5)	cip10-9
	10.3(8.5)	cip20-5
	10.3(7.5)	rsp_cip20-3
	11.0(3.5)	cip11-4
	11.0(4.5)	cip21-3
	11.0(3.5)	rsp_cip21-2
	11.1 any version	cip12-x
		cip22-x
		rsp_cip22-x

CIP2 5.x	10.2(13), 10.3(13)	cipp20-8
	11.0(10)	cipp21-7
	11.1(5)	cip22-6
	11.1(6)	cip22-7
	11.2(1)	cip22-10

1. The Cisco 7500 series requires CIP hardware revision 4.4 or later.

Table 3 Minimum Recommended CIP Boot ROM Versions

Platform and Processor	CIP Boot ROM Version	Processor ROM Monitor Version
Cisco 7000 family router[1] with a Route Processor (RP), 7000 Series Route Switch Processor (RSP7000), RSP1, and RSP2	Version 1.6 or later (required)	System Bootstrap Version 11.0 or later

1. The Cisco 7000 family routers include the Cisco 7000, Cisco 7010, Cisco 7505, Cisco 7507, and Cisco 7513.

CIP and RP/RSP DRAM Requirements

For the Cisco routers to take advantage of the Cisco IOS Release 11.2 CIP features, you might need to upgrade code, main system, or CIP memory. For specific Cisco IOS-related memory requirements, refer to the *Release Notes for Cisco IOS Release 11.2* publication (Document Number 78-2886-xx), which is available on Cisco Connection Online.

CIP Microcode Upgrade Overview

Following is an overview of how to upgrade unbundled CIP microcode (CIP Microcode Version 22.0 and later) for the Cisco 7000 family routers.

Note In the following procedure, a Cisco IOS Release 11.2 (or later) image is booted *before* the CIP microcode image is copied to Flash memory.

For CIP microcode images that were shipped on floppy disks or were obtained from CCO, do the following:

Step 1 Upload the CIP microcode image (and the Cisco IOS image if not on ROM) from the floppy disks or from CCO to a TFTP server.

Step 2 Remove any configuration commands that specify a CIP microcode image from the running configuration.

Step 3 Save your running configuration to a TFTP server or Flash memory.

Note If you have a Cisco 7000 series router and plan to install new software ROM with Cisco IOS Release 11.2 or later, skip Steps 4 and 5 and turn off power to your router. Install the new ROMs, then proceed to Step 6.

Step 4 Before you **copy tftp** you need to rename the microcode you downloaded from CIP22-3.TAR to CIP22-3. If you do not rename the microcode image, the RSP does not find the kernel because it will be named CIP22-3.TAR_kernel... instead of CIP22-3_kernel....

Step 5 Download the Cisco IOS Release 11.2 image to Flash memory.

Step 6 Configure the router to boot from the Flash memory where the Cisco IOS Release 11.2 image resides.

Step 7 Boot the Cisco IOS Release 11.2 image.

Note The router must be running Cisco IOS Release 11.2 before copying the CIP image to Flash memory in the following step because the CIP image must be "exploded" from the single image file on the TFTP server to multiple files in Flash memory. This capability is added in Release 11.2.

Step 8 Download the CIP microcode image to the Flash memory card in slot 0.

Step 9 Perform a microcode reload.

Step 10 Restore the running configuration with the configuration you saved to the TFTP server in Step 3.

For CIP microcode that shipped on Flash memory cards, do the following:

Step 1 Insert the Flash memory card into a Flash memory card slot 0.

Step 2 Configure the router to boot from the Flash memory card in slot 0.

Note For the specific procedures associated with the steps in this overview, refer to the companion publication *Upgrading Software and Microcode in Cisco 7000 Family Routers* (Document Number 78-1144-xx), which includes the information and procedures necessary to upgrade your CIP microcode. The *Upgrading Software and Microcode in Cisco 7000 Family Routers* publication includes information on upgrading software and microcode images, transferring files to and from Trivial File Transfer Protocol (TFTP) servers, copying files between nonvolatile random-access memory (NVRAM) and Flash memory, and between TFTP servers and Flash memory. The publication also includes basic instructions for booting your system.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: `http://www.cisco.com`.
- Telnet: `cco.cisco.com`.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact `cco-help@cisco.com`. For additional information, contact `cco-team@cisco.com`.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or `tac@cisco.com`. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or `cs-rep@cisco.com`.

Cisco Connection Documentation

Cisco documentation and additional literature are available on a CD called Cisco Connection Documentation, Enterprise Series. The CD is updated and shipped monthly, so it might be more up to date than printed documentation. To order the Cisco Connection Documentation, Enterprise Series CD, contact your local sales representative or call Customer Service. The CD is available both as a single CD and as an annual subscription. You can also access Cisco technical documentation on the World Wide Web URL `http://www.cisco.com`.

The complete caveats against this release are available on the Cisco Connection Documentation, Enterprise Series CD.

This document is to be used in conjunction with the *Release Notes for Cisco IOS Release 11.2* publication.

965R