Channel Interface Processor and Channel Port Adapter Microcode Release Note and Microcode Upgrade Requirements

Dec. 28, 2006
Text Part Number OL-1951-26

Contents

This document provides cumulative information for the Channel Interface Processor (CIP) and Channel Port Adapter (CPA) unbundled microcode software releases. Much of the same microcode information and procedures apply to both the CIP and CPA hardware, including the caveats in this document. Where differences do occur, they are noted and identified as applicable to either the CIP or CPA.

This release note includes the following topics:

- Introduction, page 2
- How to Obtain Microcode, page 2
- System Requirements, page 3
- Upgrading the CIP and CPA Microcode, page 9
- Caveats for CIP and CPA Microcode, page 11
- Related Documentation, page 139
- Obtaining Documentation, page 143
- Documentation Feedback, page 144
- Cisco Product Security Overview, page 144
- Product Alerts and Field Notices, page 145
- Obtaining Technical Assistance, page 146
- Obtaining Additional Publications and Information, page 147
Introduction

This section provides some background information on the CIP and CPA microcode and upgrade guidelines.

The CPA includes the Enterprise Systems Connection (ESCON) CPA and the Parallel CPA. The ESCON CPA (ECPA) and Parallel CPA (PCPA) are additions to the Cisco Mainframe Channel Connection (CMCC) family of adapters, which also includes the Channel Interface Processor (CIP) and CIP2. The CPA microcode runs on both the ECPA and the PCPA. Cisco IOS Release 11.3(3)T and later supports the ECPA. Cisco IOS Release 11.3(7)T and later and Cisco IOS Release 12.0(1) and later support the PCPA. Cisco IOS Release 12.1(5)T and later supports the ECPA4.

Note
Throughout the remainder of this document, CPA is used to refer to both the ECPA and PCPA. The ECPA and PCPA are no longer produced.

Any given Cisco IOS software release attempts to load a default level of the microcode software for the CIP and CPA. Prior to Cisco IOS Release 11.1 for the CIP, the microcode software was only available within the Cisco IOS software bundle.

In Cisco IOS Release 11.1 and later, the microcode became available unbundled from the Cisco IOS software. Therefore, you must obtain the microcode as a separately loadable software module.

There is a default setting in the Cisco IOS software that corresponds to a particular level of microcode that is already loaded on the router Flash memory card (or on the SanDisk memory device for the CPA) when you purchase a CIP or CPA with a system. But, if you order a CIP or CPA as a spare (shipped separately from a system), you might be required to download the microcode image from Cisco.com.

If you need to load a version of the microcode independently, you should be sure you are running a compatible version of the Cisco IOS software. For information about microcode and Cisco IOS software compatibility, see the “Hardware and Software Compatibility” section on page 3.

Caution
If you are upgrading from a release prior to Cisco IOS Release 11.1, a special microcode installation procedure is required or your CIP will not operate properly. For details, refer to the section “Upgrading the CIP and CPA Microcode” section on page 9.

How to Obtain Microcode

When the CIP or CPA hardware is shipped as part of a system order, you will receive a copy of the Cisco IOS software image and the microcode software preinstalled on a Flash disk or Sandisk device.

When your order the CIP or CPA hardware as a spare that is not part of a system order, or if you want to upgrade your microcode, then you need to obtain the microcode from Cisco.com.

System Requirements

This section provides important information about hardware and software requirements.

CIP RSP and CPA Cisco 7200 DRAM Requirements

For the Cisco Systems routers to take advantage of the CIP and CPA features in the Cisco IOS software, you might need to upgrade code, main system, or CIP/CPA memory. For specific Cisco IOS-related memory requirements, refer to the Cisco IOS software release note publications corresponding to your Cisco IOS software release. For a list of the related Cisco IOS software publications, refer to the “Release-Specific Documentation” section on page 140.

Hardware and Software Compatibility

This section provides Cisco IOS software, microcode, and ROM monitor software compatibility information for your CIP and CPA hardware and processor modules. It includes the following topics:

- Cisco IOS Software and Microcode Guidelines, page 3
- Cisco IOS Software and Microcode Compatibility, page 4
- Cisco IOS Software and Hardware Compatibility, page 7
- Processor Module ROM Monitor Compatibility, page 8

Cisco IOS Software and Microcode Guidelines

When identifying an appropriate microcode version and compatible Cisco IOS software release, you should consider the following important guidelines:

- Any given Cisco IOS software release is associated with a default microcode version. A list of the current Cisco IOS software releases and the default microcode versions associated with them are provided in Table 2 on page 5. The router automatically attempts to load the default microcode version from slot 0.
- You are not required to load the default microcode version associated with a Cisco IOS software release. However, if the default microcode version is not located in slot 0, you will receive the “Failed to load cip microcode” error message. For more information, see the “Upgrading the CIP and CPA Microcode” section on page 9.
- Any given Cisco IOS software release is compatible with the microcode version that it loads by default, and any higher versions of that microcode release. Therefore, we recommend that you load the latest microcode version available within the microcode release that your Cisco IOS software supports. To determine the microcode release level required by a given Cisco IOS software release, see Table 1 on page 4.
- If you need to upgrade to a new microcode release level (for example, you need to move from release 27 to release 28 of the microcode), then you should install the latest version of release 28 microcode and also the latest available Cisco IOS release associated with microcode release 28. See Table 1 on page 4.
- The CIP and CPA hardware also require certain minimum Cisco IOS software releases. To verify these minimum requirements, see Table 3 on page 7 and Table 4 on page 7.
System Requirements

Note

The End of Engineering (EOE) and End of Sales (EOS) dates for CIP and CPA microcode releases are now associated with the EOE and EOS dates for their associated Cisco IOS software releases. For example, when the EOE for Cisco IOS Release 12.0 is announced, the EOE for microcode release 26 will also occur. The product bulletin providing information about Cisco IOS software release dates and milestones is available at http://www.cisco.com/warp/customer/cc/pd/iosw/iore/prodlit/367_pb.htm. (To access this bulletin, you must have a valid Cisco.com account and be logged in.)

Cisco IOS Software and Microcode Compatibility

This section provides information about compatibility between microcode versions and Cisco IOS software releases for the Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series routers. The CIP and CPA microcode images are shipped in a bundle separate from the Cisco IOS software images.

Required Microcode Releases for Cisco IOS Software

Table 1 provides a list of the microcode releases that are required for each of the currently available Cisco IOS software releases. For example, if you are running any version of the Cisco IOS Release 12.0 mainline software, then you must run release 26 of the CIP/CPA microcode. If you are running any release of Cisco IOS Release 12.0 T or Cisco IOS Release 12.1 T prior to Cisco IOS Release 12.1(5)T, then you must run release 27 of the microcode. Cisco IOS Release 12.1(5)T and later supports microcode release 28.

Table 1  Cisco IOS Software and CIP/CPA Microcode Release Requirements

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Required Microcode Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3 T</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.3</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.2S</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.2 T</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.2</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.1 T</td>
<td>27-xx</td>
</tr>
<tr>
<td>12.1</td>
<td>27-xx</td>
</tr>
<tr>
<td>12.1E</td>
<td>27-xx</td>
</tr>
<tr>
<td>12.0 T</td>
<td>27-xx</td>
</tr>
<tr>
<td>12.0</td>
<td>26-xx</td>
</tr>
<tr>
<td>12.4</td>
<td>28-xx</td>
</tr>
<tr>
<td>12.4T</td>
<td>28-xx</td>
</tr>
</tbody>
</table>

1. New commands and features were introduced for the CIP and CPA in Cisco IOS Release 12.1(5)T and release 28 of the microcode. Therefore, release 27 of the microcode is required for any Cisco IOS 12.1 T releases prior to Cisco IOS Release 12.1(5)T, and release 28 is required at Cisco IOS Release 12.1(5)T and later.
If you plan to upgrade to a new microcode release level (such as from 27 to 28), then we recommend that you obtain both the latest microcode release level and the latest Cisco IOS release available for that microcode. For example, if you are running Cisco IOS Release 12.1 supporting microcode release 27 level, and you plan to upgrade to microcode release 28 level, then you should also install Cisco IOS Release 12.2(16), or the latest Cisco IOS 12.2 release or Cisco IOS 12.2 T release available at the time that you upgrade. Otherwise, you might not receive the full feature and command support for that microcode release.

### Default Microcode Versions Loaded by the Cisco IOS Software

Every Cisco IOS software release is associated with a default microcode version. Table 2 provides a list of each of the available microcode versions (organized by release level) and the corresponding Cisco IOS software releases that load that microcode version by default. Recall that you are not required to load the default microcode version associated with a Cisco IOS software release. For more information about microcode and Cisco IOS software guidelines, see the “Cisco IOS Software and Microcode Guidelines” section on page 3.

It is important to recognize that the router attempts to load the default microcode version from slot 0. If the default microcode version is not located in slot 0, you will receive the “Failed to load cip microcode” error message. Therefore, if you are loading a different microcode version or you are loading the microcode from a location other than slot 0, be sure that you configure the appropriate microcode command and specify the corresponding microcode filename and location. For more information, see the “Upgrading the CIP and CPA Microcode” section on page 9.

The XCPA microcode became available in Release 26.

### Table 2 Default Microcode Versions for Cisco IOS Software Releases

<table>
<thead>
<tr>
<th>Default Microcode Version (CIP/ XCPA)</th>
<th>Loaded automatically from slot 0 by the following Cisco IOS software releases:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microcode Release 28:</strong></td>
<td></td>
</tr>
<tr>
<td>28-18</td>
<td>12.2(27), 12.3(12), 12.4(1), 12.2(27)S</td>
</tr>
<tr>
<td>28-14</td>
<td>12.2(21), 12.2(23), 12.2(20)S</td>
</tr>
<tr>
<td>28-12</td>
<td>12.2(16), 12.2(17)S</td>
</tr>
<tr>
<td>28-11</td>
<td>12.2(12), 12.2(13), 12.2(12)S</td>
</tr>
<tr>
<td>28-10</td>
<td>12.2(10), 12.2(11)S</td>
</tr>
<tr>
<td>28-9</td>
<td>12.2(7)</td>
</tr>
<tr>
<td>28-8</td>
<td>12.2(5), 12.2(6)S</td>
</tr>
<tr>
<td>28-6</td>
<td>12.2(3), 12.2(2)S</td>
</tr>
<tr>
<td>28-5</td>
<td>12.2(1), 12.2(2)T, 12.2(1)S</td>
</tr>
<tr>
<td><strong>Microcode Release 27:</strong></td>
<td></td>
</tr>
<tr>
<td>27-26</td>
<td>12.1(22), 12.1(22)E</td>
</tr>
<tr>
<td>27-23</td>
<td>12.1(18), 12.1(19), 12.1(20), 12.1(21), 12.1(19)E</td>
</tr>
</tbody>
</table>
### System Requirements

<table>
<thead>
<tr>
<th>Default Microcode Version (CIP/XCPA)</th>
<th>Loaded automatically from slot 0 by the following Cisco IOS software releases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>27-22</td>
<td>12.1(16), 12.1(17)</td>
</tr>
<tr>
<td>27-21</td>
<td>12.1(14)</td>
</tr>
<tr>
<td>27-20</td>
<td>12.1(12), 12.1(12)E</td>
</tr>
<tr>
<td>27-19</td>
<td>12.1(11), 12.1(11)E</td>
</tr>
<tr>
<td>27-18</td>
<td>12.1(10)</td>
</tr>
<tr>
<td>27-17</td>
<td>12.1(9)</td>
</tr>
<tr>
<td>27-16</td>
<td>12.1(8)</td>
</tr>
<tr>
<td>27-13</td>
<td>12.1(7)</td>
</tr>
<tr>
<td>27-11</td>
<td>12.1(6)</td>
</tr>
<tr>
<td>27-9</td>
<td>12.1(4), 12.1(4)T</td>
</tr>
<tr>
<td>27-8</td>
<td>12.1(3), 12.1(3)T</td>
</tr>
<tr>
<td>27-7</td>
<td>12.1(2), 12.1(2)T</td>
</tr>
<tr>
<td>27-6</td>
<td>12.1(1), 12.1(1)T</td>
</tr>
<tr>
<td>27-5</td>
<td>12.1(1), 12.1(1)T</td>
</tr>
<tr>
<td>27-4</td>
<td>12.0(7)T, 12.0(8), 12.0(8)T, 12.0(9), 12.0(9)T</td>
</tr>
<tr>
<td>27-3</td>
<td>12.0(7)</td>
</tr>
<tr>
<td>27-2</td>
<td>12.0(5)T, 12.0(6)</td>
</tr>
<tr>
<td>27-1</td>
<td>12.0(4)T, 12.0(5), 12.0(6)</td>
</tr>
<tr>
<td>27-0</td>
<td>12.0(3)T, 12.0(4), 12.0(5)</td>
</tr>
</tbody>
</table>

**Microcode Release 26:**

<table>
<thead>
<tr>
<th>Default Microcode Version (CIP/XCPA)</th>
<th>Loaded automatically from slot 0 by the following Cisco IOS software releases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-31</td>
<td>12.0(28)</td>
</tr>
<tr>
<td>26-29</td>
<td>12.0(26), 12.0(27)</td>
</tr>
<tr>
<td>26-28</td>
<td>12.0(25)</td>
</tr>
<tr>
<td>26-27</td>
<td>12.0(23), 12.0(24)</td>
</tr>
<tr>
<td>26-26</td>
<td>12.0(22)</td>
</tr>
<tr>
<td>26-25</td>
<td>12.0(20)</td>
</tr>
<tr>
<td>26-24</td>
<td>12.0(19)</td>
</tr>
<tr>
<td>26-23</td>
<td>12.0(18)</td>
</tr>
<tr>
<td>26-21</td>
<td>12.0(17)</td>
</tr>
<tr>
<td>26-20</td>
<td>12.0(16)</td>
</tr>
<tr>
<td>26-19</td>
<td>12.0(16)</td>
</tr>
<tr>
<td>26-18</td>
<td>12.0(15)</td>
</tr>
<tr>
<td>26-17</td>
<td>12.0(14)</td>
</tr>
<tr>
<td>26-16</td>
<td>12.0(13)</td>
</tr>
<tr>
<td>26-15</td>
<td>12.0(12)</td>
</tr>
</tbody>
</table>
**Table 2**  
**Default Microcode Versions for Cisco IOS Software Releases (continued)**

<table>
<thead>
<tr>
<th>Default Microcode Version (CIP/ XCPA)</th>
<th>Loaded automatically from slot 0 by the following Cisco IOS software releases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-13</td>
<td>12.0(11)</td>
</tr>
<tr>
<td>26-12</td>
<td>12.0(10)</td>
</tr>
<tr>
<td>26-11</td>
<td>12.0(9)</td>
</tr>
<tr>
<td>26-10</td>
<td>12.0(8)</td>
</tr>
<tr>
<td>26-9</td>
<td>12.0(6), 12.0(7)</td>
</tr>
<tr>
<td>26-8</td>
<td>11.3(10)T, 11.3(11)T, 12.0(5)</td>
</tr>
<tr>
<td>26-7</td>
<td>11.3(9)T, 12.0(4)</td>
</tr>
<tr>
<td>26-5</td>
<td>11.3(8)T, 12.0(3)</td>
</tr>
<tr>
<td>26-4</td>
<td>11.3(7)T, 12.0(1), 12.0(2), 12.0(1)T, 12.0(2)T</td>
</tr>
</tbody>
</table>

**Cisco IOS Software and Hardware Compatibility**

Table 3 lists the minimum Cisco IOS software releases and the corresponding default microcode versions that are available for CIP Version 5 hardware.

**Table 3**  
**Minimum Cisco IOS Software Releases for CIP Hardware Version 5**

<table>
<thead>
<tr>
<th>CIP Hardware Version</th>
<th>Minimum Cisco IOS Release</th>
<th>Default Microcode Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP2 Version 5.x</td>
<td>12.3(1)T</td>
<td>cip28-2</td>
</tr>
<tr>
<td></td>
<td>12.3(1)</td>
<td>cip28-2</td>
</tr>
<tr>
<td></td>
<td>12.2(1)T</td>
<td>cip28-2</td>
</tr>
<tr>
<td></td>
<td>12.2(1)</td>
<td>cip28-2</td>
</tr>
<tr>
<td></td>
<td>12.1(1)T</td>
<td>cip27-5</td>
</tr>
<tr>
<td></td>
<td>12.1(1)</td>
<td>cip27-5</td>
</tr>
<tr>
<td></td>
<td>12.0(1)T</td>
<td>cip26-4</td>
</tr>
<tr>
<td></td>
<td>12.0(1)</td>
<td>cip26-4</td>
</tr>
</tbody>
</table>

Table 4 lists the minimum Cisco IOS software releases and the corresponding default microcode versions that are available for the different CPA hardware versions.

The ECPA and PCPA are at End of Sale (EOS).

**Table 4**  
**Minimum Cisco IOS Software Releases by CPA Hardware Version**

<table>
<thead>
<tr>
<th>CPA Hardware Version</th>
<th>Minimum Cisco IOS Release</th>
<th>Default CPA Microcode Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECPA4</td>
<td>12.3(1)T</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td></td>
<td>12.3(1)</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td></td>
<td>12.2(1)T</td>
<td>xcpa28-2</td>
</tr>
</tbody>
</table>
System Requirements

Table 4 Minimum Cisco IOS Software Releases by CPA Hardware Version (continued)

<table>
<thead>
<tr>
<th>CPA Hardware Version</th>
<th>Minimum Cisco IOS Release</th>
<th>Default CPA Microcode Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(1)</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td></td>
<td>12.1(5)T</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td>CPA</td>
<td>12.1(1)T</td>
<td>xcpa27-5</td>
</tr>
<tr>
<td></td>
<td>12.1(1)</td>
<td>xcpa27-5</td>
</tr>
<tr>
<td></td>
<td>12.0(1)T</td>
<td>xcpa26-4</td>
</tr>
<tr>
<td></td>
<td>12.0(1)</td>
<td>xcpa26-4</td>
</tr>
<tr>
<td>ECPA</td>
<td>12.2(1)T</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td></td>
<td>12.2(1)</td>
<td>xcpa28-2</td>
</tr>
<tr>
<td></td>
<td>12.1(1)T</td>
<td>xcpa27-5</td>
</tr>
<tr>
<td></td>
<td>12.1(1)</td>
<td>xcpa27-5</td>
</tr>
<tr>
<td></td>
<td>12.0(1)T</td>
<td>xcpa26-1</td>
</tr>
<tr>
<td></td>
<td>12.0(1)</td>
<td>xcpa26-1</td>
</tr>
</tbody>
</table>

Processor Module ROM Monitor Compatibility

The ROM monitor (system bootstrap) versions for the CIP platform processor modules (RSP), as well as the ROM monitor versions for the Cisco 7200 series platform for the CPA, are typically independent of the Cisco IOS system software images. However, the CIP and CPA hardware do have minimum recommended microcode versions for each Cisco IOS software release. For more information, see the “Cisco IOS Software and Hardware Compatibility” section on page 7.

Table 5 provides the minimum CIP boot ROM and ROM monitor versions supported by router platform and processor type.

Table 5 Minimum Recommended CIP Boot ROM and ROM Monitor Versions

<table>
<thead>
<tr>
<th>Platform and Processor</th>
<th>Processor ROM Monitor Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7000 series Route Switch Processor (RSP)</td>
<td>System Bootstrap Version 11.0 or later</td>
</tr>
<tr>
<td>Cisco 7500 series router with RSP1, RSP2, RSP4/4+, RSP8, and RSP16</td>
<td>System Bootstrap Version 11.0 or later</td>
</tr>
</tbody>
</table>

Table 6 provides the minimum processor ROM monitor versions supported by the CPA.

Table 6 Minimum Recommended ROM Monitor Versions for the CPA

<table>
<thead>
<tr>
<th>Platform and Processor</th>
<th>Processor ROM Monitor Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7200 router</td>
<td>System Bootstrap Version 11.1 CA or later</td>
</tr>
</tbody>
</table>

Table 6 Minimum Recommended ROM Monitor Versions for the CPA

<table>
<thead>
<tr>
<th>Platform and Processor</th>
<th>Processor ROM Monitor Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7200 router</td>
<td>System Bootstrap Version 11.1 CA or later</td>
</tr>
</tbody>
</table>
Upgrading the CIP and CPA Microcode

Before you begin, read the “Cisco IOS Software and Microcode Guidelines” section on page 3 to be sure that you are installing a compatible Cisco IOS software and microcode version.

Note

It is important to recognize that the router attempts to load the default microcode version from slot 0. If the default microcode version is not located in slot 0, you will receive the “Failed to load cip microcode” error message. For a list of the default microcode versions automatically loaded by the Cisco IOS software, see Table 2 on page 5. When you are loading a different microcode version than the default, or you are loading the microcode from a location other than slot 0, be sure that you configure the appropriate microcode command and specify the corresponding microcode filename and location. Read the guidelines and procedures in this section for more information.

This section includes the following topics:
- Microcode Upgrade Configuration Guidelines, page 9
- Microcode Upgrade Procedure, page 10
- Microcode Command Examples, page 10

Microcode Upgrade Configuration Guidelines

Consider the following guidelines as you configure your router to load CIP/CPA microcode:

- Be sure to download the microcode image in binary format. Verify that the file size on the FTP download site matches the file size that you have downloaded.

- In some Cisco IOS releases, the CPAs in Cisco 7200 series routers using SanDisk storage media fail to load default microcode from the SanDisk. If you are using a SanDisk on the CPA, then the Cisco IOS software image must support the SanDisk. For more information, refer to the field notice at http://www.cisco.com/en/US/partner/products/hw/modules/ps2033/products_field_notice09186a0800a6908.shtml.

- If you are using a microcode image other than the default for your Cisco IOS software image, or you are copying the image to a location other than slot 0, use one of the following microcode commands:
  - For the CIP—`microcode cip flash slot:x:cip nn-nn`, where x is the slot number, and nn-nn is the microcode release that you plan to load.
  - For the CPA—`microcode ecpa {slot:y:cpa nn-nn | disk:y:cpa nn-nn}`, where y is the slot or disk number, and nn-nn is the microcode release that you plan to load. Use the disk: argument when you are loading from a SanDisk.

- When you configure the microcode command, the command line interface (CLI) parser automatically adds the microcode reload command.
Microcode Upgrade Procedure

To upgrade CIP/CPA microcode from an image obtained on Cisco.com, complete the following steps:

**Step 1**
Download the microcode image from Cisco.com to a TFTP server.

**Step 2**
Copy the microcode image to the Flash memory card in slot 0 or slot 1, or to the SanDisk memory device in disk 0 or disk 1.

**Step 3**
Save your running configuration to a TFTP server, Flash memory, or SanDisk memory device.

**Step 4**
Configure the microcode global configuration command.

The microcode command should point to the microcode image that you stored in the Flash memory card in slot 0 or slot 1, or in the SanDisk memory device in disk 0 or disk 1.

**Step 5**
Load the new microcode by completing one of the following steps:

- To reload only the updated microcode, use the microcode reload global configuration command.
- To reload the microcode from a specific slot on a Cisco 7200 series router, use the microcode reload privileged EXEC configuration command.
- To reload the updated microcode and the entire router configuration, use the reload privileged EXEC command.

For more detailed information on the procedures to upgrade the CIP microcode, refer to the companion publication *Upgrading Software and Microcode in Cisco 7000 Family Routers* (document number 78-1144-xx). The *Upgrading Software and Microcode in Cisco 7000 Family Routers* publication includes information on upgrading software and microcode images, transferring files to and from TFTP servers, copying files between NVRAM and Flash memory, and between TFTP servers and Flash memory. The publication also includes basic instructions for booting your system.

For more detailed information on upgrading the CPA microcode image, refer to the following publications:

- **PA-1C-E ESCON Channel Port Adapter Installation and Configuration**
- **PA-4C-E 1-Port High Performance ESCON Channel Port Adapter Installation and Configuration**
- **PA-1C-P Parallel Channel Port Adapter Installation and Configuration**

Microcode Command Examples

This section provides a few examples of the microcode command when loading CIP or CPA microcode from different memory devices.

**PCMCIA Examples**

The following example specifies loading the cip28-12 microcode release from Flash slot0 for the CIP:

```
Router(config)# microcode cip flash slot0:cip28-12
```

The following example specifies loading the xcpa28-12 microcode release from Flash slot0 for the CPA:

```
Router(config)# microcode ecpa slot0:xcpa28-12
```
SanDisk Example

The following example specifies loading the xcpa28-12 microcode release from disk1 on a SanDisk for the CPA:

Router(config)# microcode ecpa disk1:xcpa28-12

Caveats for CIP and CPA Microcode

Caveats describe unexpected behavior in the CIP and CPA microcode. This section provides a list of the most serious open caveats for the previous release, and resolved caveats in the current release of CIP and CPA microcode.

This section includes caveats for the following releases:

- Microcode Release 28 Caveats, page 11
- Microcode Release 27 Caveats, page 44
- Microcode Release 26 Caveats, page 96

Note
The XCPA microcode became available in Release 26.

Microcode Release 28 Caveats

This section describes the open and resolved caveats for microcode release cip28 and xcpa28. The caveats listed apply to only the most serious problems.


This section describes possible unexpected behavior in Version 28.24. All the caveats listed in this section are resolved in Version 28.25.

- Clients connecting via TN3270 SSL are randomly disconnected by the CIP Router. The issue was seen only with TN3270 SSL configured.
  The workaround is to move TN Clients to NON-SSL. [CSCse44399]

- The TN3270 server lu-seeds whose first character is numeric are rejected because they are not valid SNA names.
  The workaround, to allow the initial numeric, is to configure:
  **tn-parameter code 21** [CSCsg03731]

- Cisco CMCC configured for CMPC LLC might fail due to a buffer shortage. The local major node for one side of the connection is inactive while the other side is attempting to connect.
  The workaround is to configure the link to use the CSNA feature rather than CMPC. [CSCse91888]

- A VTAM USSMSG that is too large to fit on a 24x80 screen might cause the CMCC tn3270 server to fail. A VTAM USSTAB entry used by the TN3270 Clients was configured incorrectly as explained in IBM APAR II12568.
  The workaround is to modify the USSTAB so that it fits on a 24x80 screen. Correct the misconfigured VTAM USSTAB entry per IBM recommendations in APAR II12568. [CSCsf26598]
- A Cisco CMCC running CMPC+ might reload unexpectedly if the mainframe forwards a malformed IP packet. The failure occurred while testing security issues on the MVS system. The open source suite ISIC was being used to flood the VIPA address with malformed TCP packets. The workaround is to apply the fix for IBM APAR PK26843 to the mainframe TCP/IP stack. [CSCsg89060]

- A Cisco CMCC tn3270 server with SSL clients might reload unexpectedly. The ECPA4 was configured for TN3270 SSL and was being R-MAC’d into SNASwitch. It is not known at this time if any of these conditions had an effect or was the cause of the crash.

There is no workaround. [CSCsh19847]


This section describes possible unexpected behavior in Version 28.23. All the caveats listed in this section are resolved in Version 28.24.

- The CIP console commands `tn3270 resources`, `tn3270 scan`, and `tn3270 stats` may produce incorrect output if multiple commands are issued very quickly, for example, by pasting in multiple commands. The workaround is to allow the previous command to complete displaying its output before entering a new command. [CSCsc79152]

- Version 28-24 is required to be able to use the ECPA4 with the NPE-G2. If an older release is used, the symptom is that all IP packets to the CMCC IP stack are dropped due to an invalid checksum. There is no workaround. [CSCsd58468]

- CIP/xCPA CLAW packing trace entries do not show sufficient information to diagnose activation problems. This occurs under all conditions. There is no workaround. [CSCsd96288]

- CIP/xCPA CLAW packed activation fails under unknown conditions. There is no workaround. [CSCsd96278]


This section describes possible unexpected behavior in Version 28.22. All the caveats listed in this section are resolved in Version 28.23.


This section describes possible unexpected behavior in Version 28.21. All the caveats listed in this section are resolved in Version 28.22.

- Customers are unable to access target applications via CIP Tn3270. Tn3270 Capture Trace indicates that NO PUs are available for usage, as shown here:
This issue is seen when the CIP Card is low in memory. The following is output from the `show controller cbus` command,

```
Load metrics: Memory dram 1794472/32M ...
```

The workaround is to ensure that memory installed in CIP card can handle the current workload. A microcode reload or an OIR on the affected CIP card that is running low in memory can be used to recover the memory in the affected CIP card. [CSCsb70794]

- TN3270 clients cannot connect to CIP/ECPA TN3270-server listen-point after a change is made to the number of the clusters in a pool under a PU. This occurs when the change is made when the number of clusters allocated to the pool in the PU is at the limit on LUs. Specifically, if the pool as at the limit and the following is issued:
  ```
  no allocate lu 1 pool TEST clusters 5
  allocate lu 1 pool TEST clusters 5
  ```
  Then clients may fail to connect. This affects both LUs in the TEST pool as well as the LUs remaining in the generic pool (unassigned LUs).

  The workaround is to reactivate the affected PUs. This can be accomplished either by a VTAM `VARY INACT/ACT` or by a `shutdown | no shutdown` of the PUs. [CSCei70033]

---

Open Caveats in Version 28.20/Resolved Caveats in Version 28.21

This section describes possible unexpected behavior in Version 28.20. All the caveats listed in this section are resolved in Version 28.21.

- Under very heavy load, a Cisco Channel Interface Processor, CIP2, or Channel Port Adapter, ECPA or ECPA4, might unexpected disconnect an LLC2 session.
  
  The problem only occurs when LLC2 dynamic windowing, `llc2 nw N`, is configured and an LLC2 REJ frame is received.
  
  The workaround is to remove the `llc2 nw N` command. [CSCeh50081]

- The CIP/xCPA `llc badns` command is erroneously reporting LLC sessions that did not experience the badns condition. This causes one to believe that an LLC session had a problem when it did not. If an `llc` session experiences the badns condition, subsequently disconnects, and the control block representing that session is reused, the new LLC session shows as having experienced a badns condition in the output of the CIP/xCPA `llc badns` command.

  There is no workaround. [CSCeh51794]

- CIP/CPA LLC sessions disconnect with FRMR. This occurs when a customer runs a very heavy traffic load on the CIP/CPA and retransmissions occur.

  There is no workaround. [CSCeh75068]

This section describes possible unexpected behavior in Version 28.19. All the caveats listed in this section are resolved in Version 28.20.

- The Channel Interface Processor (CIP) running microcode cip27-29 crashes with Fatal Error (code=35) if the following command is entered without specifying a logical unit name:

  Router# % tn3270 stats lu

  The workaround is to specify a logical unit name as a parameter on the command. [CSCeg31452]

- When shutting down the TN3270 server, a fatal error 35 may be experienced. This occurs after failure of a DLUR link.

  There is no workaround. [CSCdz27554]

- SNA PUs cannot connect to VTAM through an CSNA/XCA connection. The CIP/CPA displays the following message:

  %MSG802-6-LLC_DUP_CCB: LLC Station : RMAC=4000.7507.0002 LMAC=4000.7507.0001 LSAP=04 RSAP=0C

  It might not be possible to reactivate a PU after it has been inactivated on the mainframe.

  This problem occurs after a PU 2.1. That is, a PU that uses XID format 3 attempts to connect to VTAM and VTAM rejects the connection. This could be a transient condition, if, for example, the PU’s Switched Major Node (SWN) was not active yet. When VTAM rejects the connection, it sends back an XID containing a Control Vector 22 (XID Negotiation Error) containing a sense code. The CIP or CPA mis-handles the XID containing the CV22, and places the PU’s MAC/SAP four-tuple into an invalid state. When subsequent connection attempts are made, the CIP/CPA finds the MAC/SAP four-tuple already in use and displays the %MSG802-6-LLC_DUP_CCB message. This prevents the PU from connecting.

  The workaround is to take the following action:

  1. Re-configure the PU to point to a different MAC or different CIP/CPA router.
  2. Reload the microcode.
  3. Reload the router. [CSCeg46357]

- The following message may be seen from a CMCC adapter:

  %ECPA4-6-MSG: slot2 %MSG802-6-LLC_DUP_CCB: LLC Station : RMAC=4043.3333.9000 LMAC=4041.2222.001F LSAP=08 RSAP=88

  This message occurs when very many tn3270 PUs are configured.

  There is no workaround. [CSCeg74214]

- When the CMPC+ connection is activated, the following message may be seen:

  %CIP2-3-MSG: slot1 %MPC-3-CMPCP.CV.ERR1: Unrecognized/Unexpected CV: 040C

  The problem was reported after the mainframe operating system was upgraded to z/OS R1.5. The control vector 040C contains a list of supported functions and was added for IPV6 support on the mainframe. The CV is ignored on the CIP.

  There is no workaround. [CSCeg84750]

This section describes possible unexpected behavior in Version 28.18. All the caveats listed in this section are resolved in Version 28.19.

- When many LUs are nailed to the same IP address, the client can see a long delay in getting a connection. This only happens when there are a large number of LUs nailed.
  
  The workaround is to use hsma xca-query-interval XXX. After this change, hsma xca-query-interval XXX is correct.[CSCef73273]

- Unable to issue the command hsma xca-query-interval XXX (where XXX is the desired query interval between 1-300 from the CIP console) to change the XCA query interval from the default of 30 seconds. The above command is rejected as being not valid.

- Below CMCC messages might be observed when TN3270 services stopped and started. The messages are: CMCC-4-CFGFAIL and CMCC-3-CFGCMDDROPPED: Config queue is full, command was dropped.

- The following message may be displayed on a client screen:

  THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.

  Printers may print garbage characters. This will occur when a client IP has had 10 consecutive connect failures. This "feature" was added to prevent the CIP from wasting resources on answering a TN3270 client which was asking for an unavailable VTAM resource. There have been problems with this operation with printer servers where multiple printers may appear as the same client IP address. A customer requests a way to disable this feature.

  There is no workaround. [CSCdr32459]
• The Cisco CSNA virtual token-ring adapters respond to an LLC TEST frame with a DISC frame if the SAP is not open. The correct behaviour is to ignore the TEST.
There is no workaround. [CSCef66551]

• The CIP2 Fatal Error logout is sometimes truncated. It ends after the display of "lowcore".
[CSCee42880]

• A 7200 router with a PA-4C-E XCPA Port Adapter may incur a Fatal Error 35 Error code causing the XCPA adapter to reload. The IOS being run at the time was 12.2(10b) with XCPA microcode level 28-11.
There is no workaround. [CSCef05612]

• Channel interface processor got Fatal error 37 after the channel interface shut down to recover OSPF routes. CONFIG-3-WORKLEFT: Work pending on work queue when device terminated
There is no workaround. [CSCef28648]

• The CIP/xCPA running microcode cip27-29 will crash with Fatal Error (code=35) if the following command is entered without specifying a logical unit name:
% tn3270 stats lu
The failure only occurs if a logical unit name is not entered.
The workaround is to specify a logical unit name as a parameter on the command. [CSCeg31452]


This section describes possible unexpected behavior in Version 28.17. All the caveats listed in this section are resolved in Version 28.18.

• CIP core dump utility does not always work. When the CIP crashes, no useful content of the CIP memory can be dumped, so it is impossible to determine the root cause of the crash.
There is no workaround. [CSCee17767]

• The TN3270-server allows a client to acquire LUs outside of the range specified in the client nailing statement. The problem only occurs if the client specifies a specific LU name that is outside of the valid nailed range. If the client specifies "generic", then connection is not allowed to LUs outside the nailed range. Problem was caused as a result of the resolution for ea70079, and therefore only occurs in CIP/CPA releases 28-15, 28-16 and 28-17.
There is no workaround. [CSCee18021]

• Issuing HSMA DISPLAY from the cip console shows under HSMA Configured Peers Local state: Standby. This indicates the adapter should be in a "disabled" state until an event occurs to place it in an "Active" state. In this "disabled" state the adapter should not respond or transmit any MAC frame with the HSMA MAC adapter address. When using HSMA in a PU4/5 to PU4/5 network design the Standby adapter sends a TEST frame to the target device, accepts the positive response, then sends an XID. If communications was already established with the Active adapter a DISC will occur resulting in the tear down of the original established circuit. This behavior can be verified by going into the CIP Console. Verify that the adapter is in Standby by issuing the HSMA DISPLAY command. Then performing a CIP LLC TRACE (procedures can be found on CCO). This will show the two HSMA adapters communicating between themselves over an LLC session using SAP EC. When Standby Adapter's XCA is activated you'll see the LLC TEST being source by the Standby adapter MAC address.
There is no workaround. [CSCee97867]
• A fatal error 35 may occur when a PU with LU pools already present. This problem will occur if any of the LUs (associated with the new PU) have the same name as the previously added LU pool. LU names are created based on the first 6 characters of the PU name and appending a 2 digit (hex) locaddr. If this results in a name which is the same as an LU pool name, then this fatal error 35 will occur.

To workaround this problem, do not define pool names and PU names which are the same in the first 6 characters. If the pool and PU names happen to be the same in the first 6 characters, then lu-seed should be used on the PU definition so that the LU names created won’t be the same as any pool name. [CSCee32607]

• %XCPA-3-STATUS: bay [x] Fatal error detected (code=35) %ECPA4-0-MSG: slotx %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

Immediately following a NO SHUT on the channel interface, the ECPA4 encountered a fatal error and dumped.

There is no workaround. [CSCee40253]

• TN3270-server sends up many Signal Request-to-Send (RTS) RUs to VTAM causing a VTAM hot IO condition. A client, for unknown reasons, generated many IAC Breaks (or IAC IPs - Interrupt Process) which the TN3270-server converted into Signal Request-to-Send (RTS) RUs. At the same time the CIP/xCPA sent LSA flow_off to VTAM preventing it from sending the Signal +RSPs back to the TN3270-server. This caused the VTAM IOBUF pool to be exhausted. Either the ATTN key (which generates an IAC IP) or the Break key (which generates an IAC Break) will potentially cause this problem. Note: Each type of TN3270 client will map different key sequences to generate those TN3270 command sequences.

Workaround: Specifying MAXSLOW=15-30 (seconds) in the VTAM XCA major node will cause VTAM to terminate the PU if it remains in this flow off condition more than the time period. This will prevent the excessive IO from impacting VTAM. This only applies when the PU connects to VTAM via an XCA major node. [CSCef08617]

• A 7206vxr router with a PA-4C-E XCPA Port Adapter may incur a Fatal Error 35 Error code causing the XCPA adapter to reload.

There is no workaround. [CSCef05612]


This section describes possible unexpected behavior in Version 28.16. All the caveats listed in this section are resolved in Version 28.17.

• If a c7000 has a CIP card configured with many tn3270 server PUs, when the channel x/2 interface is shut (to allow a backup CIP to take over operation), IOS may issue the following message:

%CIP2-3-MSG: slot0 %MSG802-3-HARD_ERROR: cls_cip_term: Cleanup takes too long-force takedown

The workaround is to issue a "microcode reload" to ensure that the CIP ucode integrity is restored. [CSCee03080]

• A Cisco Mainframe Channel Connection (CMCC) configured for CSNA might reload with a Fatal Error 35 if the connected mainframe stops responding. These conditions are necessary to see the problem: The CMCC is configured for CSNA. The virtual interface is started then shutdown. The connected mainframe stops responding without shutting down the CSNA device. [CSCee03619]
• 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 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.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and 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. [CSCee35335]

Open Caveats in Version 28.15/Resolved Caveats in Version 28.16

This section describes possible unexpected behavior in Version 28.15. All the caveats listed in this section are resolved in Version 28.16.

• The Tn3270 PUs in a WAIT state. The Virtual Channel Interface is in a Down/Down condition.

Messages seen in the log: TN3270S-0-ILLEGAL_CCMUTEX_RELEASE: CIP2 slot1 : Releasing unacquired semaphore,lock_held 800A9C4C lock_value FFFFFFFF ccMutex tcb 8010FCD0 thread 81459CB0

The Tn3270 PUs were hung and the Customer Shut/No Shut the Virtual Channel interface in an attempt to recover. The PUs would not recover.

The workaround is to reload the CIP Microcode. [CSCeb82536]

• In a Cisco 7500 router with a CIP2, the CIP2 may crash with a fatal error 32. The problem also may occur on a Cisco 7200 with an XCPA.

The problem may occur when a channel interface with CSNA(s) is shutdown or when a CSNA is unconfigured.

There is no workaround. [CSCec77620]

• %CIP2-6-MSG: slotx %ADAPTER-6-LOGOUT: ESCON dump output is followed by the %DEBUGGER-0-FATAL_ERROR: Fatal error (code=37) dump.

The write subchannel receives a HSCH or a CSCH while the read subchannel is waiting for access to the channel. This will only occur with very heavily utilized claw packing channels.

This behavior was observed with a feature of a mainframe TCP/IP stack that stopped and restarted a packed CLAW connection. The stack restarted the CLAW connection when there was no input from the CMCC.

The workaround is to avoid stopping packed CLAW links while there is traffic. [CSCed18702]

• If HSMA is configured on a Cisco Channel Adapter, the MAC address of a virtual adapter might be displayed incorrectly by the HSMA console command. The displayed MAC address will contain 6 extra “F”s if an odd (first, third, etc.) digit of the address is 8 or greater.

The problem is only in the display of the MAC address. [CSCed37522]
PU activation is intermittent. Sense Code 10160004 will occur. The PU will eventually activate.
This occurred when running CIP28.14 and TN3270 configured with PUs defined.
There is no workaround. [CSCed38274]

- The message: SCB limit on port NN reached, correlator: NNNN task: NAME XXXXXXXXX. might be seen for a Channel interface, CIP2 or XCPA.
  Many CSNA definitions are removed or shutdown.
  The workaround is to reload the microcode on the interface. [CSCed42343]

Open Caveats in Version 28.14/Resolved Caveats in Version 28.15

This section describes possible unexpected behavior in Version 28.14. All the caveats listed in this section are resolved in Version 28.15.

- The customer was having problems connecting to PUs performing Inverse DNS nailing. The client was getting rejected with a device type/unknown error. [CSCea70079]

- A TN3270 client will not receive the VTAM USSMSG10 screen or get a LOGAPPL session when its current LU-LU session ends if the DLUR/DLUS connection has failed and restarted during the active LU-LU session. This problem will only occur on TN3270 clients that are actively in session when/if a Backup DLUS takes over.

  There is no work around. If the client disconnects from the LU and reconnects it will get a USSMSG10 or LOGAPPL session. [CSCec04176]

- Router started getting %ADAPTER-6-LOGDATA error then the CIP crashed with a Fatal Error 37. [CSCec07315]

- The customer reports tn3270 clients are slow, or failing to connect to the tn3270 server in CIP/CPA. Tn3270 is configured on CIP/CPA.

  The workaround is to identify the client that is requesting a larger number of sessions and not completing the three-way handshake and use an ACL to filter. A temporary workaround would be to shut and no shut the Tn3270 or a specific PU identified as the clients destination IP address. [CSCec16766]

- The CIP/xCPA TN3270-server PUs go into ACT/BUSY state for extended periods of time. Eventually the PUs recover and return to ACTIVE state without any intervention. Another symptom is that LUs may go into P-NTF states. The PUs and/or LUs may enter the hung states when the upstream LLC2 link enters local busy state. This is due to TN3270-server keeping buffers that it received from the upstream link until the client acknowledges them with a TCP level ACK. This occurs with both TN3270-server DLUR PUs and direct PUs.

  There is no workaround. [CSCec57475]

- TN3270-server will allocate an LU to a TN3270 client even if the LU has never been unbound from VTAM. This can lead to session setup failures with sense code 0805000B - Session limit exceeded.
  This is known to occur under the following conditions:

  TN3270-server is configured with:
  - DLUR
  - lu termination termself
  - lu deletion never - This is the default
  - Multiple upstream links
- Application that the LU is in session with is not on the DLUS host
- RESETLU=NO is coded on LU or LUGROUP definition in VTAM (this is the default)

It also can happen for any reason where the DLUS host cannot/does not notify the application host of the termself.

The workaround is to specify RESETLU=YES causes VTAM to DACTLU/ACTLU the LU and notify the application host to send the UNBIND. This will prevent the problem. [CSCec58447]

- The XCPA/CIP experiences a Fatal Error 35. A TN3270 server PU configured with all dynamic LUs can put the TN server in a loop. When the client is trying to connect to the dynamic LU for the very first time, the LuCb is not yet created, and this was putting the server in the loop. This affects only cip/xcpa with microcode version 27-25.

In the customer's environment, they had dynamic LUs configured under all the PUs. And after they brought up the tn3270 server, after a microcode reload, the client tried connecting to those LUs.

There is no workaround. [CSCec59077]

- Part of the output of the Channel Interface Processor, CIP, console command tasks— CPU(1/5/60/busy): 1% 1% 0% 82%—is misleading. "Busy" includes time that will be used when there is other work to be done.

The workaround is to Disregard "busy". [CSCec62591]

- The TN3270-server DLUR controlled LU logon fails with either sense 80140003 or 087D0001. Topology on DLUS shows an ENDPT TG as OPER when in fact it is no longer operational. CIP/xCPA TN3270-server DLUR with multiple end point transmission groups (TGs). TN's DLUR name (CP name) must be greater in the collating sequence than the CP name of the DLUS.

The workaround is to determine the TG that is really not operational but is listed as operational on the DLUS host and delete it.

On the DLUS host issue:

D NET,ADJCP,ID=dlur_name,E - From this get the TG number from the IST1106I message. This is the current TG. D NET,TOPO,ORIG=dlur_name,DEST=dlus_name - This command should list out more than one operational (OPER) TG including the one that was shown in the D NET,ADJCP... command. Find the OPER TG that was not the current TGN,FNET,TOPO,ORIG=dlur_name,DEST=dlus_name,TGN=tg_number,FUNCTION=DELETE [CSCec70608] A CIP/XCPA adapter configured for CSNA may run out of memory over time. You may see the following error message posted in the router log when the memory has been exhausted.

%CIP2-6-MSG: slot0 %CTA-6-INACT_FREEMEM: Free Memory: 0x00090FE8
%CIP2-6-MSG: slot0 %CTA-6-INACT_SLOWDOWN: Slowdown Rcvd: Yes, 180001 ms
%CIP2-6-MSG: slot0 %CTA-6-INACT_SLOWDOWN: Slowdown Sent: Yes, 5089667 ms
%CIP2-6-MSG: slot0 %CTA-6-INACT_SCBS: SCBs in SLC: 128
%CIP2-6-MSG: slot0 %CTA-6-INACT_FLOW_COUNTS: Flow stop.resume 224/221
%CIP2-6-MSG: slot0 %CTA-6-INACT_ATTN_STATE: Attention FSM state: READ PENDING
%CIP2-6-MSG: slot0 %CTA-6-INACT_FLOW_QUEUED: Flow Resume queued in CTA: 0
%CIP2-6-MSG: slot0 %MSG802-6-FLOW_OFF_COUNT: On 505, Off<30 0, Off>30 0, total 505, max off time 0 ms

A buffer may be orphaned when an LLC2 session is terminated due to the T1 timer expiring N2 times.
The workaround is to issue a "microcode reload" command to free up the memory on the CIP/XCPA. [CSCec76268]

- The CIP/xCPA TN3270 Server converts USSSCS USSMSGs to 3270 datastreams for TN3270E clients even if they have negotiated the SYSREQ function.

The TN3270 client must negotiate TN3270E and the SYSREQ function without negotiating the BIND-IMAGE function.

There is no workaround. [CSCed12577]

- CIP microcode unexpectedly reloads with fatal error 35. This is a rare occurrence that can happen if a tn3270 client is disconnected during the processing of data to that client.

There is no workaround. [CSCed18618]

- The HSMA_LINK_STATE message contains an extra "now". Dec 9 07:32:13.092: %ECPA-6-MSG: slot2 %MSG802-6-HSMA_LINK_STATE: The hsma-partner link 4000.0000.0001 is now now unresolved.

This is a cosmetic issue. [CSCed19774]


This section describes possible unexpected behavior in Version 28.13. All the caveats listed in this section are resolved in Version 28.14.

- A deactivate LU (DACTLU) operation on an LU in the middle of a multi-LU cluster pool could render the entire cluster unusable. The same is true if the statically defined LU is not available on the host, but is configured on the router in the middle of a cluster. When this occurs, the client is not granted connection beyond the faulty LU.

There is no workaround. [CSCdr95560]

- Prior to CIP and CPA microcode version 28.14, the CPAs were not supported on the Cisco 7200 series routers with the NPE-G1.

The workaround is to use the ECPA4 (PA-4C-E) with the NPE-G1 using microcode version 28.14. The ECPA (PA-1C-E) and PCPA (PA-1C-P) are not supported with the NPE-G1. [CSCea27903]

- When we inactivate an XCA major node in VTAM, VTAM has sent DACTPU commands and received DACTPU ACKs to/from all of the TN3270 server PUs. However, some TN3270 server PUs may not become inactive and subsequently cannot be activated. When this occurs, the TN3270 server PU status (shown using the show extended channel tn3270-server command) remains as “P-ACTPU” or “ACT-BUSY”.

The workaround is to run the shut and noshut commands at the PU scope, which properly activates any PUs that are suspended in this condition. [CSCea47302]

- If you configure the router for CLAW packing but do not change the TCPIP profile, then the following message might be seen:

Mar 17 07:49:18 EST: %CIP2-6-MSG: slot0 %PACK-6-RANGE2: Out of range sublink (64) received in packed claw message.

Prior to CIP and CPA microcode version 28.14, the error message does not identify the host that is sending the invalid frames. There is no workaround.

With microcode version 28.14, the CLAW packing error messages include the path and device address to identify the connection on which the error is being generated. [CSCea52705]
• If a CMPC connection from an OS host is inactivated by VTAM (the local major node PU is inactivated), then the router log reports the following message:

CIP2-3-MSG: slot5 %MPC-3-BAD_HDR: Unrecognized MPC header received: 0000C000 00000000

The CIP does not clear the LLC2 connection. Therefore, the upstream link remains connected. CMPC is not processing the DISCONNECT request from VTAM, so the LLCC (MPC LLC) connection is left in a bad state preventing the subsequent attempts to activate the LLC connection from completing.

This problem does not exist between the CIP and OS/390 systems.

The workaround is to reconfigure the connection using CSNA or CMPC+. [CSCea71612]


This section describes possible unexpected behavior in Version 28.12. All the caveats listed in this section are resolved in Version 28.13.

• Print jobs through an Open Connect print server are sometimes suspending.

This is occurring when the host application fails to send an End Bracket Indication (EBI) to the Secondary Logical Unit (SLU, which is the printer) prior to unbinding the session. The EBI triggers the TN3270 server to send IAC-Abort Output (AO) to the client that indicates the print job is complete. In the absence of EBI, the IAC-AO is not sent to the printer, and the print does not complete.

With the fix, the CMCC TN3270 server sends AO (Abort Output) to non-E printers or End of Job (EOJ) for E-printers when it is in receive state (in bracket in the outbound direction) when the TN3270 server receives an UNBIND. This will force data previously written to the printer to be printed.

There is no workaround. [CSCdp72090]

• Change the CIP code to flip the direction bit in the Routing Information Field (RIF).

Because the CIP code does not use the direction bit in the RIF like the Network Control Program (NCP), it can cause confusion when you use CiscoWorks Blue Maps to display information. In CiscoWorks, the RIF map is shown backward. This problem should be specific to CiscoWorks Blue Maps and under normal LLC/SNA operation, this should not cause any issue.

There is no workaround. [CSCdv46342]

• A Cisco Mainframe Channel Connection (CMCC) router with a CIP or CPA that is configured for TN3270 server and Secured Socket Layer (SSL) encryption might restart with a fatal error 09.

When the TN3270 server uses SSL, the data stream contains xFF characters. The Telnet protocol requires that xFF characters in the data stream be doubled to xFFFF. If the data in the request/response unit (RU), after doubling the xFF characters, exceeds the 4K buffer size, then the fatal error might occur.

Workarounds are to disable SSL, or possibly use an RU size less than 2048 bytes. [CSCdx08946]

• The output from the show extended channel tn3270-server dlur command shows the CP-CP status as NOTKNOWN.

This problem occurs if there is more than one DLUR-DLUS link to the Network Node Server (NNS) and the CP-CP session is not on the first link in the router configuration.

There is no workaround. [CSCdx39152]

• CCA-0-DEV_ERR2: Device error but no active defined device.
The CIP or CPA crashes with DEBUGGER-0-FATAL_ERROR, unexpected reload with fatal error code=37. The CIP or CPA receives a frame from the host mainframe, but due to a logic error in the ESCON chipset on the CIP and CPA, it is not handled correctly. The CIP or CPA detects the logic error in the chipset and forces a microcode reload with a fatal error.

There is no workaround. [CSCdz31806]

- The output from the `show extended channel tn3270-server pu` command displays the LU as inactive while the VTAM display from the command `d net,id=nnnnnnn,n,e` (where `nnnnnnn` is the LU name) shows the LU as unstable.

The client connects to the TN3270 server and TN3270 sends a Notify Available to VTAM. If the client disconnects while TN3270 is still waiting for the Notify response, and if the response is not received in a predefined timeout, the described symptom can occur. This is because TN3270 puts the LU in reset state without notifying VTAM. TN3270 now has the LU as being inactive while VTAM thinks it is active, but unstable. An attempt to inact/act the LU at this point results in the LU being stuck in the PDACL state in VTAM.

There is no workaround. [CSCdz36410]

- A fatal error 35 might occur on the CIP or CPA when you issue a command from within the TN3270 server configuration prompt.

The fatal error 35 is observed when the `no listen-point` command is issued as shown in the following example, where `xxx.xxx.xxx.xxx` is the IP address of the listening point:

```
no listen-point xxx.xxx.xxx.xxx
```

There is no workaround. [CSCdz38654]

- The CIP TN3270 server advertises its MAX I-FIELD=4105 during XID negotiation even though the RIF indicates the MAX frame is 1500 bytes.

When sending an XID, the value being reported for the maxIField (bytes 10-11 in XID) might be too large if the previously received RIF from a test packet indicates a lower value. The TN3270 server should be comparing its MaxIField from the SAP with the MaxDataRoute (received from the link-station partner via Test/RIF), and report the smaller of the two when sending the XID.

There is no workaround. [CSCdz38697]

- Under certain circumstances when the TN3270 server is configured for DLUR, it can misinterpret the SLU name it receives if the PCID includes x4B in the received bind request. The LU-LU session is unbound with sense code 8004 0000.

In this situation, the TN3270 server is configured as DLUR. The DLUS returns the SLU name not network qualified. The PCID contains x4B.

There is no workaround. [CSCdz48129]

- The CIP ucode could fail with a fatal error 35 if the `tn3270 option debug N` command is started from the CIP console with `N ≥ 7` and SSL is running.

There is no workaround. [CSCdz65261]

- The status of the LU in VTAM is PSESEND-P, while the LU state on the router is ACT/NA.

This problem can occur if a client is bound to an application, but has entered the SSCP session (via system request key) to make a request. In this case, the TN3270 server thinks that the client is waiting to be bound to some other application. If the client disconnects while in this state, the server goes into a “waiting for bind” condition and ignores a subsequent unbind (because the server incorrectly thinks that the LU is not currently bound). When VTAM receives no response to the unbind, the LU is placed into the PSESEND state.
Caveats for CIP and CPA Microcode

There is no workaround. Once the condition is observed, you must cycle the LUs in VTAM. [CSCdz69040]

- The TN3270 server on a CIP or CPA might run out of memory. This occurs when the TN3270 server is configured for Secured Socket Layer (SSL) encryption.

There is no workaround. [CSCdz73605]

- When a client connects to an LU, the LU will sometimes suspend in a P_NTF/UA state as shown in the following sample output from the show extended channel tn3270-server pu command:

```
Router# sh ext chan 5/2 tn3270-ser pu PUNAME
.
lu    name   client-ip:tcp        nail  state
2   RA5V0202 10.61.4.102:44291     N   ACT/SESS
3   RA5V0203 10.43.8.86:2642       N   P-NTF/UA
```

This problem is the result of a small timing window when a client connects to an LU (logical unit) before that LU session has completed the cleanup from a previous client connection.

The workaround is to deactivate the LU at the host and reactivate it. [CSCdz75177]

- A Cisco Mainframe Channel Connection (CMCC) router with a CIP or CPA that is configured for TN3270 server and Secured Socket Layer (SSL) encryption might encounter hung or dropped client sessions.

When the TN3270 server uses SSL, the data stream contains xFF characters. When this error occurs, the data passed to TCP/IP is larger than 4096 bytes.

Workarounds are to disable SSL, or possibly use an RU size less than 2048 bytes. [CSCdz79681]

- A TN3270 TCP/IP session to a Cisco CMCC TN3270 server might hang. The hang will occur on a non-SSL session after a “transient write failure”—a shortage of TCP send buffer space. To trigger the problem, an SSL session must be started to the TN3270 server. This problem occurs on all CMCC 28-x releases.

A Cisco Mainframe Channel Connection (CMCC) router with a CIP or CPA that is configured for TN3270 server and Secured Socket Layer (SSL) encryption might encounter hung or dropped client sessions. TN3270 is configured for both SSL and non-SSL sessions. An SSL client session encounters a transient shortage of TCP/IP buffer space. Non-SSL clients might hang.

There is no workaround. [CSCea00167]


This section describes possible unexpected behavior in Version 28.11. All the caveats listed in this section are resolved in Version 28.12.

- The CIP does not clean up properly after VTAM or an XCA major node is recycled. The following error messages appear in the router log:

```
6:43:13.323: %ECPA-6-MSG: slot1 %MSG802-6-LLC_DUP_CCB: LLC Station :
RMAC=4000.4000.0002 LMAC=4000.4000.2222 LSAP=04 RSAP=C6
```

Note The following workaround might lead to a CIP microcode reload, and should only be performed if a CIP microcode reload is a tolerable side effect.
The workaround is to issue the `shut` command followed by the `no shut` command while in TN3270 PU configuration mode. This seems to clear the physical unit (PU) condition, and the PU goes to active status. [CSCdr90542]

- TCP connections for TN3270 clients might remain in the close-wait state indefinitely after a client disconnects.

This problem only occurs if the client happens to disconnect while the LU (logical unit) is in the state of waiting for ACTLU (activate LU). This might occur if the LU group major node is not active, or if ACTLU is slow to arrive. If the client reconnects, a new TCP connection would be opened while the old connection remains in close-wait. The new connection will operate normally.

There is no workaround. [CSCdx01730]

- Performance improvements for the CIP and CPA.

You might see any number of symptoms that might be impacting overall system performance. First, you might see many RDBs (Read Dropped Blocks) as shown in the output from the `show extended channel statistics` command. In the following example, `xxx` is the number of read dropped blocks caused by a temporary (normal) condition of no memory buffers available for queueing to the mainframe:

```
Router# show extended channel 1/0 statistics
```

<table>
<thead>
<tr>
<th>Dev</th>
<th>Connects</th>
<th>Retries</th>
<th>Cancels</th>
<th>Selective</th>
<th>System</th>
<th>Device</th>
<th>CU</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This particular condition has been aggravated by the addition of the Gigabit Ethernet NIC feeding the CIP as an ingress network port. Additional symptoms might be noticed by a large amount of overhead in the CMPC Plus channel I/O packets sent to the mainframe.

---

**Note**

CMPC Plus users should refer to IBM APAR/PTF PQ61503/AQ61503 prior to installing this level of microcode (or subsequent levels of microcode). Refer to this APAR to find the appropriate sysrouted APAR for your OS release due to data corruption issues found on the IBM mainframe.

There is no workaround. [CSCdx72717]

- The number of LUs in the output from the `show extended channel tn3270-server` command varies when nailing is configured on the CIP or CPA.

This example sets up 5 LUs in the host. The TN3270 server is configured on the CPA without nailing. The output from the `show extended channel tn3270-server` command shows 10 LUs:

```
Router# sh extended cha 4/0 tn
```

```
server-ip:tcp     <current stats>  < connection stats >  <response time(ms)>
server-ip:tcp     lu  in-use  connect  disconn  fail  host  tcp
10.0.0.23:23      10   0       0         0         0     0      0
```
However, when you configure nailing, the output from the `show extended channel tn3270-server` command shows 5 LUs:

```
Router# sh extended cha 4/0 tn

server-ip:tcp    <current stats>  < connection stats >  <response time(ms)>
10.0.0.23:23:23  5               0        0        0     0      0      0      0

There is no workaround. [CSCdx93118]
```

- The CIP or CPA interfaces that are configured for CLAW can get fatal error 37.

  The fatal error 37 can appear after the following messages:

  `%%%BSQ-0-SCB_CHAIN: CIP2 slot4 : Read SCB chain is out of sequence`
  or
  `%%%ADAPTER-6-LOGOUT: CIP2 slotX : Port N logout data. Adapter microcode C50602D4`

  The mainframe syslogs will show channel errors for the devices. The fix allows for additional
  error-checking conditions so the ESCON code can recover and not take a fatal error.
  There is no workaround. [CSCdy06181]

- A CIP running TN3270 might experience memory leaks in the TN3270 response time task which
  eventually takes down the CIP with a fatal error 37:

  `%CIP2-3-MSG: slot1 %CBUS_ATTN-3-DUMPUCODE: Dump of the CIP microcode has been
  requested CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=37)`

  There is no workaround. [CSCdy10459]

- The CIP or CPA might crash with a fatal error 35 in Aluc_Start_SscpLu.

  This is a very rare occurrence due to a small timing window when a client might disconnect while
  some other event (host packet processing) is in progress. This could incorrectly leave the LU (logical
  unit) in the LU-LU session state, even though the client has disconnected. The result is that upon
  receiving subsequent packets (such as BIND, UNBIND), the server attempts to reference data
  structures that have been freed, resulting in the fatal error.

  There is no workaround. [CSCdy20175]

- Unused Cisco Multipath Channel Transmission Group (CMPC TG) connections might lead to a
  buffer shortage in the CIP or CPA. The result is that no CMPC TGs will be able to reconnect once
  disconnected. This has been observed on a CPA running xcpa26-26 microcode.

  The workaround is to disable the host PUs (physical units) associated with the CMPC TG to stop
  the buffer leak root cause, and then to issue a microcode reload to recover the lost buffers. Another
  workaround is to remove any unused CMPC TGs from the router configuration. [CSCdy44696]

- LLC_DUP_SAP, fatal error 9 in ssi_buff.c, or PUs in P-ACTPU state due to a buffer loss condition.
  It is possible that other errors (such as ACT/BUSY on PUs) could occur as a result of this buffer loss.

  The TN3270 buffers that are used to communicate to the LLC layer are being lost, which eventually
  results in a depletion of the buffers and can cause any of the errors mentioned above. This buffer
  loss can occur during a link close or disconnect operation, such as would occur during a “shut” of
  TN3270, a listen-point or PU. A buffer is lost for each PU doing the close or disconnect operation.

  The buffer pool that is getting depleted is shown in the “tn3270 stats” (in the CIP or CPA console).
  The second line from the bottom of the stats output is referred to as the “DLUR inbound pool free
  buffers.” The title is misleading as these buffers are also used for direct PUs.
The following example shows the normal number of free buffers (150) in the DLUR inbound pool. When this buffer pool is low or depleted, the problems mentioned above can occur:

```
LStn Svcs inbound pool free buffers 520
DLUR inbound pool free buffers 150 etcetera...
```

There is no workaround. [CSCdy46286]

- Host print jobs are getting stuck on a CIP router configured for TN3270 server using SSL encryption. This problem is with SSL-defined TN3270 PUs only. The problem usually occurs directly after seeing the following error message in TN3270 trace output:

  TCP write had transient failure

A possible workaround is to lower the RU size of the print job down to 1 Kb. [CSCdy63889]

- The CIP Dumps with a fatal error 35 in RcvDACTxU.

  A deactivate LU (DACTLU) packet is being received to an LU (logical unit) that the DLUR application does not currently have defined. DLUR should be rejecting the DACTLU with sense code 08120007 rather than crashing with a fatal error.

  There is no workaround. [CSCdy85034]

- When using the NetSolve application on the mainframe to query the CIP for TN3270 LU names, you might see the LU name display as a blank or the LU name might be incomplete.

  The error is only seen on applications that use the TN3270 Monitor interface to the CMCC TN3270 server.

  The workaround is to use the Cisco IOS `show extended channel tn3270-server` command to display LUs. [CSCdz15898]

### Open Caveats in Version 28.10/Resolved Caveats in Version 28.11

This section describes possible unexpected behavior in Version 28.10. All the caveats listed in this section are resolved in Version 28.11.

- If the TN3270 server rejects the Activate Logical Unit (ACTLU) with a 08970000 sense code, the LU is not properly placed in the INACTIVE state on the server (VTAM thinks the LU is inactive and the server thinks it is active). This confusion appears in the `show` command output. In future connect attempts to the LU, the server waits for LU-LU responses from the VTAM which it will not get since there is no LU-LU session. The server logs messages such as NO_BIND_REQ_RCVD and NO_NTFY_AV_RSP_RCVD.

  There is no workaround. [CSCdu40765]

- A NO_BIND_REQ_RCVD error is logged for a logical unit (LU) even though the client has already been disconnected due to a NEGOT_TIME_EXPIRED error.

  A NEGOT_TIME_EXPIRED error occurs when a client attempts a connection, and the connection takes an excessive amount of time to complete, due to an Activate LU (ACTLU) not being received in a timely manner. When the logical unit (LU) to which the client is attempting to connect to finally receives an Activate LU (ACTLU), the TN3270 server puts the LU in the P-BIND state although the client has already disconnected. Because the client is disconnected, the server does not send the Notify/available inbound for the LU, and a NO_BIND_REQ_RCVD is logged.
There were no effects other than the logging of the NO_BIND_REQ_RCVD message. There is no workaround. [CSCdu63277]

- After a TN3270 client disconnects, and while the disconnect processing is occurring, an inactivity timer expires on the client, forcing the TN3270 server to try to disconnect the client that is already disconnected. The following message occurs:

    %CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]: luname:72 pu:80F1A2A0,tnet:0
    %CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR_INFO: LU info: Event 16 12 3 10 4 8 18 9 18 4 8 18 17 14 20 1, state = 5, snaState = 1
    %CIP2-1-MSG: slot5 01, flag = D0

    A workaround is to disable the configuration options that would cause the client to disconnect due to inactivity, such as keepalives and idle time. [CSCdw31269]

- The CIP TN3270 server may exhibit a slow memory leak in the TN3270 server response time task. The workaround is to stop and restart the CIP TN3270 server. [CSCdw88211]

- The TN3270 server does not send an inbound NOTIFY or TERMSELF response following a NO_BIND_REQ_RCVD error.

    This could occur while an LU is in the system services control point (SSCP) state (immediately following client connection or unbind/passive) and a BIND is not received within a 2.5 minute timeout. The VTAM/CICS does not clean up, so the application currently assigned to the LU remains, and the next client to connect might get an incorrect application.

    There is no workaround. [CSCdx56737]

- A NO_BIND_REQ_RCVD error is logged for TN3270 printers and the printers disconnect.

    When a printer connects to the TN3270 server, but no print jobs are ready to be printed, the TN3270 server disconnects after 2.5 minutes and a NO_BIND_REQ_RCVD error is logged. If this occurs, subsequent printing fails because the printer is no longer connected.

    The TN3270 server should not disconnect printers when a BIND is not received within 2.5 minutes. This should only occur for LU type 2 (display) clients.

    The workaround is to verify whether print jobs are ready to be sent to the printer before connecting to the TN3270 server. [CSCdx58390]

Open Caveats in Version 28.9/Resolved Caveats in Version 28.10

This section describes possible unexpected behavior in Version 28.9. All the caveats listed in this section are resolved in Version 28.10.

- A host receives an INOP 01 code message when a logical link control (LLC) session disconnects. This problem occurs when two VTAM systems are connected through an APPN network and an operation such as a normal disconnected mode (NDM) file transfer is processed. One end of the connection terminates the operation normally. The other end detects the LLC session disconnection and forwards a close_station_indication message with a code 7657 to VTAM. The code 7657 is translated as an abnormal disconnection sequence and causes VTAM to issue a IST1412I message with a return code 7657 and an INOP code 01.
The CIP should send a normal LLC disconnection sequence indication with a code 7656 instead. This sequence is illustrated in the following example:

Hosta--cip/csna-------dlsw------cip/csna----Hostb
<----------------appn----------------------->

There is no workaround. [CSCdp12204]

- The CIP crashes with a fatal error code 35. Just before the crash, the following error message type is logged:

  bad LU on DISC: PU index is -1, LOCADDR is 216, DISC reason is 19
  ..remote IP address = 80.1.25.67, tnetSession = EE33BEAF, ipNext=0
  %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]:
    :216 pu:FF55DEAD, tnet:EE33BEAF
  %TN3270S-1-LU_ERROR_INFO: LU info: Event 9 10 20 10 16 12 10 4
    8 9 10 16 17 1 15

  This error occurs after performing a “shut” on the TN3270 server. This could occur any time the server attempts to disconnect a logical unit (LU) when the physical unit (PU) is in the process of being deleted.

  There is no workaround. [CSCdr11739]

- A CIP fatal error 35 occurs after a shutdown of the TN3270 server or the Dependent Logical Unit Requestor (DLUR) component of the TN3270 server. This problem does not occur often, but when encountered it seems related to high volume networks where the TN Server and Host are busy. In most instances, the TN Server will also log messages for the physical unit (PU) or logical unit (LU), stating it did not get a response from the Host in 30 seconds.

  The fatal error occurs after issuing the shut command from the TN server or DLUR.

  There is no workaround. [CSCdu03050]

- A NO_BIND_REQ_RCVD error is logged for a logical unit (LU) even though the client has already been disconnected due to a NEGOT_TIME_EXPIRED error.

  A NEGOT_TIME_EXPIRED error occurs when a client attempts a connection, and the connection takes an excessive amount of time to complete, due to an Activate LU (ACTLU) not being received in a timely manner. When the logical unit (LU) to which the client is attempting to connect to finally receives an Activate LU (ACTLU), the TN3270 server puts the LU in the P-BIND state although the client has already disconnected. Because the client is disconnected, the server does not send the Notify/available inbound for the LU, and a NO_BIND_REQ_RCVD is logged.

  There were no effects other than the logging of the NO_BIND_REQ_RCVD message.

  There is no workaround. [CSCdu63277]

- An AS/400 TN3270 client negotiates a termtype of IBM-3487 with the CIP TN3270 server. IBM-3487 is an invalid 3270 termtype and will not handle 3270 data streams correctly.

  This terminal type (along with similar models 3486, 3488, and 3489) should be rejected by the CIP.

  There is no workaround. [CSCdv83239]

- The TN3720 Server is not providing a response to some request/response units (RUs) which have the definite response bit(s) set (DRI1 and/or DRI2) or the pacing indicator (PI) bit set in the SNA RH. This only occurs after a message for “TCP write had transient failure” happens on the TCP/IP side of the telnet connection. If the write failure occurs on an RU that has one of these bits set or on any subsequent RU with these bits set, and that RU gets queued before a retry of the failed write, then the server will not respond to the RU. This bug only occurs in the 28-xx branch.
There is no workaround. [CSCdw16545]

- After a TN3270 client disconnects, and while the disconnect processing is occurring, an inactivity timer expires on the client, forcing the TN3270 server to try to disconnect the client that is already disconnected. The following message occurs:

```
%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]: luname:72
pu:80F1A2A0,tnet:0
%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR_INFO: LU info: Event 16 12 3 10 4 8 18 9 18 4 8
18 17 14 20 1 ,state = 5,snaState = 1
%CIP2-1-MSG: slot5 01, flag = D0
```

A workaround is to disable the configuration options that would cause the client to disconnect due to inactivity, such as keepalives and idle time. [CSCdw31269]

- The customer file transfer application reports CRC failures during the first few files transferred. Eventually, the CRC failures stopped.

This bug occurs when the customer uses an increased number of receive direct memory access (DMA) buffers for the Logical Link Control (LLC) on the CIP.

The workaround is to maintain the number of DMA buffers at the default — do not configure the max-llc2-rcvbuffs. [CSCdw55422]

### Open Caveats in Version 28.8/Resolved Caveats in Version 28.9

This section describes possible unexpected behavior by Version 28.8. All the caveats listed in this section are resolved in Version 28.9.

- The working window size (Ww), displayed by the `show extended channel x/2 llc oper` command might display 0 instead of the correct value.

There is no workaround. [CSCdt92975]

- The binds from the Network Node Server (NNS) are rejected with sense code 08150004, LFSID in use.

This problem only occurs with Dependent Logical Unit Requestor (DLUR) physical units (PUs). It then occurs when the link to the NNS goes down. For example, with a 3745 controller acting as the NNS, a customer can take the tic down on the 3745, or shut the Cisco Systems Network Architecture (CSNA) channel to the host.

The TN3270 server Dependent Logical Unit Requestor (DLUR) link failure cleanup results in a condition where the local form session identifier (LFSID) is still in use, causing future (i.e., when the link recovers) BINDs from the Network Node Server (NNS) control point to be rejected with sense 08150004. This failure to clean up the LFSIDs causes internal DLUR PU processing to improperly shut down processing of the lost links. The result is that the TN3270 server does not recover the DLUR/DLUS pipe, and the TN3270 physical unit (PUs) fail to activate.

There is no workaround. [CSCdu01381]

- ESCON CPA (ECPA) to Parallel CPA (ECPA) file transfer showed a large number, 30 percent, of retransmitted I-frames. Examination of the receiving CPA showed a large number of Read DMA Failures due to no buffers.

This bug is seen when large number of file transfers occurs simultaneously over several concurrent logical link control (LLC) sessions.

The workaround is to use a very small window size, which reduces the number of retransmits as well as overall throughput. [CSCdu24530]
If a Cisco 7500 series router with a CIP card is reloaded or the **microcode reload** command is issued, the devices on the mainframe that correspond to the Cisco Systems Network Architecture (CSNA) or the Common Link Access to Workstation (7) devices on the router might get “BOXED”. The mainframe is running OS/390. The CS/390 version is 2.8 IST11881 VTAM CSV2R8 STARTED AT 04:43:06 ON 04/08/01. This problem is observed running Cisco IOS Release 12.1(4) or Cisco IOS Release 12.1(6). The CIP microcode in use was cip27-12.

The workaround is to either have the devices varied OFFLINE on the mainframe where they are defined, or if the reload happens unintentionally (i.e., a router crash, or a power outage, etc.), vary the BOXED device OFFLINE, with the UNCOND option. [CSCdu26652]

A fatal error 9 was encountered running IP over Cisco MultiPath Channel Plus (CMPCPLUS) using the new ESCON Channel Port Adapter Version 4 (ECPA4) in a 7206VXR router with an NPE400. There is no workaround. [CSCdu49534]

An invalid Management Processor Card (MPC) buffer from the mainframe causes a fatal error 35 on the CIP. There is no workaround. [CSCdu66303]

Common Link Access to Workstation (CLAW) packing failed to initialize when using cip26-20 or above. This problem is caused by CSCds32524 where it introduced a new flag bit which only affects the CLAW feature, but the fix has not been incorporated into CLAW packing. There is no workaround. [CSCdu80489]

Multiple console messages appear when performing a CIP reload. There is no workaround. [CSCdv04228]

While booting the CIP, it might take an excessive amount of time if LU nailing is being used, and a common client IP/mask combination is nailed to many physical units (PUs). The amount of time it takes varies, depending upon how many physical units/logical units (PUs/LUs) the client mask is nailed to. It could take many minutes for hundreds of PUs, or hours if nailed to 1000 or more PUs. During this time, the CIP CPU utilization will be up around 100 percent. There is no workaround. [CSCdv17797]

The router **syslog** messages show the following just prior to a fatal error 9.

```%ECPA-3-MSG: slot4 %CMPTG-3-LS_FSM_ERR: TG Name: P2US6092-Ls, Event IslepiFlowStop, State SStationOpen %XCPA-3-STATUS: bay [4] Fatal error detected (code=9) %ECPA-3-MSG: slot4 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/ls.C @ 339 - msgP```

The cause for this is unclear. There is no workaround. [CSCdv25071]

The following message appears during Cisco SNA (CSNA) and Cisco Multipath Channel (CMPC) configuration sessions:

```%SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./mpc/mpc.C @ 5793 - msgP```

There is no workaround. [CSCdv58115]
- A Cisco router with CIP running TN3270 and Cisco SNA (CSNA) reloads with the following error messages:

```
%SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./cta802/dlu.c @ 437 - this && this->read_q && msg
%DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

There is no workaround. [CSCdv63166]

- Sense code 0812 0007 errors and/or error message 0897 are returned in response to an Activate LU (ACTLU).

This is much more likely to occur when using the dynamic logical unit (LU) naming feature. The problem is experienced if the Virtual Telecommunications Access Method (VTAM)/host is initial program loaded (IPL) without reloading the router.

The workaround is that if you IPL the host, also reload the router to clean up internal data structures. [CSCdv71737]

### Open Caveats in Version 28.7/Resolved Caveats in Version 28.8

This section describes possible unexpected behavior in Version 28.7. All the caveats listed in this section are resolved in Version 28.8.

- When a microcode reload occurs, the router log does not indicate what version of CIP microcode is being reloaded.

There is no workaround. [CSCdt82371]

- The performance for logical link control (LLC) links is greatly reduced or stopped, while the link physically remains active, but little to no data flows over the session. This occurs when the customer uses two Channel Interface Processors (CIPs) between mainframe (MF) environments. Customers have 4 xCPAs sending Main Frames (MF) data over LLC connections in a physical unit 5 (PU5) to PU5 environment, mapping many view runners (VRs) over a single LLC2 Virtual Routes (VRs) instance. Between the two CIP routers is an OC-48 pipe; the customer desires a minimum of 40M throughput and uses large local LLC windows to accomplish this end.

Due to network congestions, packets are lost between the two CIP routers causing flow control measures to be activated. As a result, the dynamic windowing support is enabled. As part of the dynamic windowing support, the local send window is reduced, and not subsequently increased per specifications.

The workaround is not to enable dynamic window support on CIP (llc2 nw). [CSCdu08352]

- The TN3270 Dependent Logical Unit Requester (DLUR) link fails to activate when the remote MAC (RMAC) is an Advanced Peer-to-Peer Networking (APPN) port on the same router. The BIND is rejected with the sense code 80040000.

The workaround is to change the RMAC to point to an external communications adapter (XCA), and not the APPN port. [CSCdu19516]

- If the TCP port is changed for a TN3270 PU, clients can no longer connect to logical units (LUs) defined on that physical unit (PU).

The workaround is to avoid reconfiguring the TCP port. [CSCdu35076]
• A router with ESCON CPA (ECPA) loses the Cisco Multipath Channel (CMPC) Transmission Group link and becomes inactive, for some unknown reason. The log displays the following:

```
%ECPA-3-MSG: slot4 %CMPTG-3-LS_FSM_ERR: TG Name: WMP1B -
Ls, Event IXidInd, State SConnected
```

The workaround is to perform a shut/no shut on the interface. [CSCdu40527]

• A CIP fatal error 35 appears when processing a configure-nack to an Inter Processor Communication (IPC) message.

There is no workaround. [CSCdu40818]

• A noticeable delay occurs when the client is connecting, and might result in the logging of a DNS failure. This occurs when configured DNS servers are unreachable, or when a client IP address cannot be found, which causes a search through multiple servers and/or retrying of DNS servers.

The workaround is to assure that DNS servers are reachable and DNS names are defined when DNS servers are being configured. To prevent delays, but not the logging of the DNS lookup failures, configure the server with the `no ip domain-lookup` command.

A noticeable delay might occur when the client is connecting, and a DNS failure might be logged. [CSCdu88459]

• Logical units (LUs), which should be free and available might not be available. Symptoms could be that “resource not found” errors are logged, or the Activate LU (ACTLU) might be rejected with an error message 0897. This problem occurs when the TN Server detects a logical unit (LU) name clash. An LU name clash might occur in the following circumstances:

  – Customers use the same first 6 characters for physical unit (PU) names without defining an `lu-seed`. The server creates default LU names by concatenating the first 6 characters of the physical name (PU) name with the `locaddr`.
  
  – Customers define static LUs (at VTAM) with names that clash with the default names on the server. For example, if the server has a PU named PU1, it will name LUs (by default) so that locaddr 1 is PU1001, locaddr 2 is PU1002, and so forth. If the static VTAM names are inconsistent so that locaddr 2 is PU1000, locaddr 3 is PU1001, and so forth, this results in a name clash on the server.

  – Customers use `dynamic lu` naming, which might produce a name clash.

**Note** Name clashes are generally acceptable. The server has an algorithm which handles the clashes by renaming unclaimed LUs to avoid the clash. There was an error in this logic which made some LUs inaccessible.

If a customer sees LU names beginning with a 4 digit decimal value (such as 0001xxxx, 0002xxxx) in the output of a `show extended channel tn3270-server pu` command or a `tn3270 resources pu` command, then the server has detected a name clash and this bug is likely.

A workaround is to avoid situations which produce name clashes such as those identified above. [CSCdv08691]

This section describes possible unexpected behavior in Version 28.6. All the caveats listed in this section are resolved in Version 28.7.

- A fatal error 35 occurs from CIP TN3270 server, when `TNSessionDisConnect` is the last entry in the trace.
  
  There is no workaround. [CSCdt24977]

- The TN3270 server is not cleaning up the logical unit (LU). The LU is being reallocated for another session, which then displays the previous login screen at the host. The router displays the following message in the above situation:

  `%CIP2-3-MSG: slot4 \%TN3270S-3-NO_BIND_REQ_RCVD:
  No BIND REQ received on LU xxx`

  There is no workaround. [CSCdt84286]

- If a particular logical partition (LPAR) on the mainframe (MF) hangs, it could cause a CIP adapter to hang and not pass traffic. This can occur when running CIP microcode Release 26-17. The CIP can hang, providing no diagnostic output to determine the condition that caused the hang.

  The customer might see the following message when this occurs:

  `%IPC_RSP_CBUS-3-NOBUF: No more IPC memd buffers to transmit IPC message.`

  This problem was seen in the following environment: CIP Release 26-17, Cisco IOS Release 12.0(9)

  **Topo:**
  
<table>
<thead>
<tr>
<th></th>
<th>MF-1</th>
<th>MF-2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>\</td>
<td>/</td>
</tr>
<tr>
<td></td>
<td>\</td>
<td>/</td>
</tr>
<tr>
<td></td>
<td>\</td>
<td>/</td>
</tr>
<tr>
<td>Escon</td>
<td>Dir1</td>
<td>Escon</td>
</tr>
<tr>
<td></td>
<td>\</td>
<td>/</td>
</tr>
<tr>
<td></td>
<td>CIP rtr1</td>
<td>CIP rtr2</td>
</tr>
</tbody>
</table>

  The CIP adapter in each CIP router hung when LPAR 4 in MF-1 hung.

  The workaround is to issue a microcode reload command and/or reload the router. We had to issue the microcode reload command two times before it took effect. [CSCdt86405]

- If the TN3270 server receives an active physical unit (ACTPU) for a physical unit (PU) that is already active, the TN3270 server is not forwarding the product set identification (PSID) packets inbound for logical units (LUs) that are active on the PU. Therefore, the LUs do not appear as active/in-session in the virtual telecommunications access method (VTAM).

  This situation might occur in cases where the TN3270 PUs are downstream from a Dependent Logical Unit Requester (DLUR) node upstream. If the DLUR link is taken down and then re-established, the only communication to the TN3270 server is a subsequent Activate Physical Unit (ACTPU). Because no intervening deactivate physical unit (DACTPU) is sent to the TN3270 server, this results in the server receiving the ACTPU while the PU is already active, thus resulting in the situation described above.

  There is no workaround. However, this bug does not appear to present any real problems other than the LUs do not appear as active in the VTAM status displays. Operationally, the LUs appear to function properly. [CSCdu30329]

- If the TCP port is changed for a TN3270 PU, clients can no longer connect to LUs defined on that PU.

  The workaround is to avoid reconfiguring the TCP port. [CSCdu35076]
Open Caveats in Version 28.5/Resolved Caveats in Version 28.6

This section describes possible unexpected behavior in Version 28.5. All the caveats listed in this section are resolved in Version 28.6.

- When the USS messages are too long, the TN3270 server does not suppress the Clear key. Instead, the TN3270 server sends it to the virtual telecommunications access method (VTAM). The VTAM answers with an error message. An inbound clear aid should be suppressed and a write with keyboard restore would be sent back to the client.

The workaround is to code shorter USS messages in the USS table. [CSCdt51737]

- The TN3270 server user logs on to a virtual telecommunications access method (VTAM) application from a USSMSG10. This application sends the BIND and then, upon receiving the BIND +RSP, sends the Start Data Traffic (SDT), and gets a response. The application then waits for the user to enter a transaction ID. It does not actually send a screen (or clear screen) to the logical unit (LU). On a locally attached LU to a 3174, the 3174 clears the screen when putting the LU into the LU-LU session (previously it was in the SSCP-LU session).

The CIP/CPA TN3270 server does not clear the screen. This leaves the screen with the USSMSG10 and USSMSG0 ("COMMAND ACCEPTED") screen displayed at the client.

The VTAM application needs to be one that does not initially write to the logical units (LUs) screen. No particular levels of IOS, CIP/CPA microcode or VTAM apply.

The workaround is to modify the application and send out an Erase/Write command to the LU. [CSCdh57583]


This section describes possible unexpected behavior in Version 28.4. All the caveats listed in this section are resolved in Version 28.5.

- Bouncing transmission groups (TGs) for Cisco Multipath Channel Plus (CMPC+) frequently causes the CIP to restart with the following messages:

```
01:40:03:%ECPA-0-MSG:slot5 %BSQ-0-SCB_CHAIN:Read SCB chain is out of sequence
01:40:03:%ECPA-0-MSG:slot5 %DEBUGGER-0-FATAL_ERROR:Fatal error (code=37)
```

This problem is found in cip27 releases.

The workaround is not to activate, then deactivate TGs frequently when traffic is running from the CIP to the mainframe. [CSCdk87042]
• The TN3270 server on the CIP might wait three seconds before sending a **notify slu enabled** message when a client requesting a nonstatic logical unit (LU) by name attempts to reconnect. The workaround is to code the LU termination as **always**. [CSCDs74621]

• When you define a new physical unit (PU) at virtual telecommunications access method (VTAM), if static logical units (LUs) and INCLUD0E=yes, the activate logical units (ACTLUs) to those static LUs might be rejected with a 0897 sense code. This error occurs when LU names from a previously defined PU are reused when defining the new PU.

The workaround is to remove the original PU (on which the LUs were named) from the PU definition on the router using the **no PU <puname>** command. [CSCdt01236]

• The Channel Interface Processor 2 (CIP2) board crashes with the following fatal error 32:

  ```
  %CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=32)
  ```

This occurs when you enter a **no pu** command on a TN3270 server.

There is no workaround. [CSCdt05019]

• If a client connects to a Logical Unit (LU) using the dynamic LU naming feature, the following type of error might occur when a user disconnects from the LU.

  ```
  %CIP2:slot3 ChangeResourceName:new name PUA01 conflicts
  ```

Once this error occurs, the LU can only be accessed by using the name given the LU by the previous dynamic LU naming client. In some situations, a fatal error, such as that described in CSCdt01019 might occur.

These problems occur when the server’s internal LU names clash, causing pseudo-names to be created. Internal names clash when the first 6 characters of a PU name on a common listen-point are the same. The server builds LU names by combining the first 6 characters of the PU name with the **locaddr**, so when the first 6 characters of the PU names are the same, the names clash.

A workaround is to define PU names in which the first 6 characters are unique, or use unique LU seeds on the PU definition on the server. If **lu-seed** is used on the server PU definitions, we recommend that the seed match the LUSEED defined for the PU in the Virtual Telecommunications Access Method (VTAM) PU definition. [CSCdt18308]

• When installing a new Common Link Access to Workstation (CLAW) packing feature, packstat, from the CIP console does not work correctly when ELPs exceed 16.

There is no workaround. [CSCdt42288]

• The customer configures a TN3270 server with a logical unit (LU) nailing and dynamic LU on a CIP. If a TN3270E client asks for a LU which is not assigned to the client, the TN3270 server should send a reject frame, as described in RFC 854. You must use dynamic LU, LU nailing, and TN3270E client for this to occur.

There is no workaround. [CSCdt44144]

• When there are too many TCP connections to a TN3270 physical unit (PU) IP address destination port 65535, the CIP processor crashes with the following messages:

  ```
  %CIP2-0-MSG: slot4 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35) 27 19:00:06:
  %CIP2-0-MSG: slot4 %SCHED-0-NOPROCID: No process id available for process creation
  %CIP2-0-MSG: slot4 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)
  ```

There is no workaround. [CSCdt47389]

• After the channel has timed out on the CIP, the following output is given:

Con should be N.
The above occurs when the channel has timed out due to the host having been stopped (i.e., “v net.cancel”).

There is no workaround. [CSCdt47430]

- An NetView Distribution Manager (NDM) data transfer was performed. When verified on the receiving end, the file contained additional records.

There is no workaround. [CSCdt70199]

- A fatal error 35 (FE35) might occur when a no listen-point command is given while sessions are active.

There is no workaround. [CSCdt73803]

Open Caveats in Version 28.3/Resolved Caveats in Version 28.4

This section describes possible unexpected behavior in Version 28.3. All the caveats listed in this section are resolved in Version 28.4.

- The CIP restarts with a fatal error 35 when configuring Cisco Multipath Channel (CMPC) statements with alternating no shut. This occurs if the following sequence is pasted in interface mode:

```
int ch2/1
    cmpc C040 72 TG0 READ
    no shut
    cmpc C040 73 TG0 WRITE
    no shut
    cmpc C040 74 TG1 READ
```

The workaround is to issue the no shut command once. [CSCdm39276]

- The Block Dropped on Read subchannel increases when trying to bring up a CLAW session while the other CLAW session is active, and the log displays the following message:

```
%CIP2-6-MSG: slot5 %SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
```

This condition occurs only under the following circumstances:

- The CIP is running out of System Control Board (SCB).
- Only one CLAW device is configured or one device was hit by a large number of packets in a short period of time.
- You are trying to bring up or tear down one more CLAW session. You should:
  1. Shut down the interface.
  2. Perform a microcode reload.
  3. Confirm that all CLAW devices are configured.
  4. Perform a no shut.
A hole in the `get_scb` function exists, where we allocate and release SCB in the same thread. Because the CIP allocates SCB for control message using this function, there is a potential CIP lock when the CIP is hit by the above conditions.

There is no workaround. [CSCds32524]

- When using VRN (Virtual Routing Node) to connect the TN3270 server to multiple hosts, the server attempts to create many dynamic links with a host, which fails, but uses up all its available dynamic link stations.

There is no workaround. [CSCds50942]

- Issuing the `lfc stat protocol all` command on the CIP console results in a fatal error 35. Without configuring any adapters, if we issue `lfc` commands on the CIP console, fatal error 35 results.

There is no workaround. [CSCdt10243]

- The TN3270 server sometimes awards a client a logical unit (LU) nailed with a shorter netmask over an LU nailed with a longer netmask. This occurs in the following two scenarios.

  In the first scenario, the user configures a new client nailing statement that has a longer netmask than an existing client nailing statement that covers the same client. If the client has been awarded LUs in the past from the shorter netmask, then newer client connections will be awarded the LUs from the shorter netmask first.

  In the second scenario, the configuration already contains two nailed client statements, one with a shorter netmask. If the client connects using different model types, occasionally the client is incorrectly awarded an LU from the nailing statement with the shorter netmask.

Following is a sample configuration problem fix:

```
    tn3270-server
    idle-time 60
    keepalive 60
    dlur NETA.JMK NETA.MVSD
    lsap token-adapter 1
    link HOSTMVSD rmac 4000.7500.7500
    pu PUL 11111111 10.100.1.1
    client ip 10.100.0.0 255.255.0.0 lu 224 225
    pu PUZ 22222222 10.100.1.1
    client ip 10.100.1.0 255.255.255.0 lu 113 114
```

Prior to this fix, a client with an IP address of 10.100.1.10 would sometimes get LU 224 or LU 225 before LU 113 or LU 114. The TN3270 server should always award a nailed LU with a longer netmask over an LU with a shorter netmask.

A workaround is to perform a shut and no shut on the TN3270 server. [CSCdt18785]

### Open Caveats in Version 28.2/Resolved Caveats in Version 28.3

This section describes possible unexpected behavior in Version 28.2. All the caveats listed in this section are resolved in Version 28.3.

- The counter displayed by the `show ext ch x/2 connection-map llc2` command displays the wrong number of active Logical Link Control, type 2 (LLC2) connections when the Virtual Telecommunications Access Method (VTAM) is configured to connect out through the CIP. The count matches the number of connections open when it should match the number of connections established.

There is no workaround. [CSCdi67144]
• The CIP Logical Link Control (LLC) WwCountChanges counter from the `show extended channel slot/port llc statistics mac sap mac sap` command, and the ConnectFail counter from the `show extended channel slot/port llc statistics` are not incrementing correctly.

There is no workaround. [CSCds29197]

• The CIP TN3270 `show extended channel x/x tn3270-server security sec-profile` command will in some instances indicate a fully loaded certificate, even though prior messages indicate it was not successfully loaded. This problem occurs when the certificate being loaded was built incorrectly. It does not occur if the certificate being loaded is not found.

There is no workaround. [CSCdt04398]


This section describes possible unexpected behavior in Version 28.1. All the caveats listed in this section are resolved in Version 28.2.

• The TN3270 server logs various messages if the TN3270 client fails to connect to the TN3270 servers on the CIP/CPA. The bug requests that the TN3270 server on the CIP/CPA send those messages to the TN3270 clients.

  **Note**  This is not a software bug. This DDTS only requests an enhancement on the TN3270 server.

The workaround is to look at the router log. [CSCdr50532]

• Clients attempting to connect to a CIP TN3270 server using pooled logical units (LUs) might receive the following message.

  **This terminal has requested a resource not known on the TN3270 server. Therefore, it is being placed into a hold state. Please contact your help desk for resolution of this problem.**

  The LUs are statically defined to VTAM and `lu-deletion never` and `lu termination termself` are coded. The LUs during the session termination process are not always returned to the pool. Eventually the pool runs out of LUs and the above message is displayed at the client.

  The workaround is to enter the following commands from the CIP/CPA console:

  ```
  if-con cip_slot c
  tn3270 option nmvt_psid 0
  if-quit
  ```

  These commands will not live through a router reload or microcode reload. [CSCdr66536]

• A fatal error 35 crash occurs on the CIP, TN3270 server, or virtual interface, shutting it down.

  There is no workaround. [CSCdr73141]

• Issuing a `tasks query` command from the CIP console with the wrong process ID number causes a fatal error 32.

  There is no workaround. [CSCdr74632]

• When the CIP receives many small packets in a very short period of time, the router freezes or locks up and receives these messages:

  ```
  %CIP2-6-MSG: slot5 %SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
  %CIP2-6-MSG: slot5 %SCB-6-RESUME: SCB on port 0 available, correlator: 0 task: CLAW read0/C700/00 8040CE10
  ```
The workaround depends on customer network topology and configuration. [CSCdr85879]

- Cisco Multipath Channel Transmission Groups (CMPC TGs) will stick in the SAttachSapPending state. This occurs if multiple CMPC TGs share the same service access point (SAP) on an adapter. Occasionally, only the TGs will get the `attachsap.cfm` message, while the other TGs will remain in the SAttachSapPending state and will not become active.

The workaround is to inactivate, then reactivate the LS major nodes for affected TGs. [CSCdr87920]

- The printer does not respond to data flow when the TN3270 server holds the keyboard restore until a `change direction` command is received. Two new options have been added to allow new keyboard restore functionality.

The following options are now available:

  - `tn-parameter code 7` — Enables functionality per CSCdm93990; the server does not manipulate keyboard restore on chained WSFs, for all type devices.
  - `tn-parameter code 11` — Server does not manipulate keyboard restore on WSF, Write, and E/W commands for printers only.
  - `tn-parameter code 12` — Server does not manipulate keyboard restore on WSF, Write, and E/W commands for displays only.

All three of the commands can be enabled to provide totally nonmanipulative keyboard restore data stream flow. Client: Attachments 6.4 and 6.5.

There is no workaround. [CSCdr93053]

- When the mainframe goes down and subchannels are still active, primarily during IPL of the mainframe, the following message is displayed:
  
  `%CTA-0-INACTIVE: PA0 CTA 8C40-C0 reset after being inactive for 180 seconds
  %RSP-3-RESTART: interface Channel4/2, output stuck
  %IPC_RSP_CBUS-3-NOBUF: No more IPC memd buffers to transmit IPC message`

The workaround is to shut down all the subchannels before IPL of the mainframe. [CSCdr95975]

- When running the offload feature on a Cisco 7500 series router with a CIP and IBM TPF mainframe, the following message is displayed:
  
  `%CIP2-4-MSG: slot0 %OFFL-4-BADDESC: Socket descriptor 3 in request is bad: state DESC_Holddown compare 3 might be encountered`

This message is a warning to show that CIP receives an offload request command for a socket which already closed or does not exist anymore. This message does not cause any negative impact to the network or the mainframe.

There is no workaround. [CSCdr98652]

- The CIP TN3270 server might produce the following message:

  `%TN3270S-6-BADTIMER: Bad timer operation(1),ra=8006AF14,funcPtr=0,oldFuncPtr=80B6E5AC`

  **Note**  The values for `ra` and `oldFuncPtr` might be different. This message can appear if the server is configured for `lu deletion termself`. Unless other problems are noted, the message might be ignored. This DDTS applies only to BADTIMER messages with operation(1).

There is no workaround. [CSCds00674]
• When using a CIP on a Cisco 7500 series router or a CPA card on a Cisco 7200 series router, the Cisco Mainframe Channel Connection (CMCC) might crash with a fatal error. This is seen only in rare situations when the free memory in the CMCC is either completely utilized or highly fragmented.

The workaround is to increase the memory on the CMCC. [CSCds05651]

• The TN3270 server sends a negative response inbound (to the host) with an incorrect sequence number field. A TN3270E printer sends a negative response to the server with a sequence number of “0”, rather than having the sequence number match the last sequence that the server sent to the client. This causes the server to send a negative response inbound (to the host) with an incorrect sequence number.

There is no workaround. [CSCds13542]

• A fatal error 35 occurs when removing the TN3270 server DLUR configuration on the shutdown virtual channel interface.

There is no workaround. [CSCds14146]

• Customers with Cisco 7000 series routers running TN3270 servers might rarely encounter a fatal error 35 as a result of an unexpected system reload.

There is no workaround. [CSCds16631]

• Previously, in legacy style configurations when a client was nailed using a client `ip a.b.c.d x.x.x.x lu` statement, the mask was applied by Cisco IOS software before being sent to the CIP. Currently, with Kirribilli-release style configurations, Cisco IOS software does not apply the mask before sending the nailing statement to the CIP, which has the following two side effects:

  1) Using masks, we can now nail the same client to different pools of logical units (LUs).

  2) Because the masks are applied by the CIP and not applied in Cisco IOS software, some client IP statements cannot be removed from configurations.

Item number one will not be addressed in this DDTS. To reproduce number two, configure the TN3270 server as follows:

tn3270-server
pool JEFFPC cluster layout 2s
listen-point 172.18.5.237
pu JJ1PU 90007424 token-adapter 15 14 rmac 7500.cafe.efef lu-seed JJ1PU###
allocate lu 10 pool JEFFPC clusters 1

Then, nail the client to pool JEFFPC with the following statement:

client ip 10.83.10.202 255.255.0.0 pool JEFFPC

Look at the nailing tables on the CIP:

Nailed address = 10.83.0.0, mask value 255.255.0.0

When you attempt to remove the nailing statement, you will receive the following message:

%TN3270-1-NAIL_NOT_FOUND: Deletion of the Client IP (10.83.10.202) LU:\Nailing first (0) to last (0) failed because the configuration was not\nfound.

Configure an alternative to the CIP as follows:

no client ip 10.83.0.0 255.255.0.0 pool JEFFPC

Cisco IOS software says:

%client ip 10.83.0.0 is not configured.
To remove the client IP statement, you must reload Cisco IOS software.
There is no workaround. [CSCds23641]

- The Channel Interface Processor Common Link Access to Workstation (CLAW) packing hangs when the CIP CLAW packing receives an Internet Protocol (IP) packet which is larger than the negotiated CLAW frame size minus the CLAW packed header size.

The workaround is to configure the IP Maximum Transmission Unit (MTU) where the size would be a negotiated packet frame size (cross check with PROFILE TCPIP definition in the mainframe) minus 4 (the packed header size). [CSCds24793]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with a fatal error 9 because a corrupted or runt MPOA Client (MPC) frame has been received.

```
%CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSL_ASSERT failure in ../mpc/mpc.C @ 2049 - ssi_msg_length( bfrP) >= (sizeof( MpcFra
%CIP2-3-MSG: slot0 memHdr) + frameSize)
%CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

There is no workaround. [CSCds27703]

- Once a logical unit (LU) is disconnected, the client cannot reconnect for 10 seconds. This happens when the tn-server, listen-point, or physical unit (PU) is configured for lu deletion never, which is the default value. After an LU disconnects, the server waits for 10 seconds for the host to respond to an inbound power-off product-set identification (PSID). However, when lu-deletion is set to “never”, no PSID request is sent inbound, so no host response will be received. The fix is to configure lu deletion always. This will force the power off PSID to be sent inbound.

There is no workaround. [CSCds28146]

- A fatal error 35 appears from the CIP TN3270 server, when the server tries to send a -RSP to a Start Data Traffic (SDT), but the client disconnects while waiting for a timing mark before sending the response.

The workaround is not to configure the timing mark under the TN3270 server scope. [CSCds31131]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with the fatal error 9 below when a virtual CIP adapter is removed that is part of an active transmission group (TG).

```
%ECPA-3-MSG: slot3 %SSI802-3-FATAL_ERROR: SSL_ASSERT failure in ../mpc/clean.C @ 372 - elemP
%ECPA-0-MSG: slot3 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

The workaround is not to remove adapters for TGs without first inactivating the TG from the host system. When defining TGs make sure all adapters are configured first. [CSCds32606]

- The NO_LU_SESSIONS message, which appears when a client requests connection to a generic logical unit (LU) when no generic LUs are available, does not contain data to indicate which client is attempting the connection. Also, after 10 such attempts, the client should be put into a hold state rather than being allowed to continually attempt the connection to an unavailable resource. The client attempts to connect to a generic LU, but no generic LUs are available.

Note: This problem has also been seen when a TG is coded using an adapter that is not currently defined.

```
%ECPA-3-MSG: slot3 %SSI802-3-FATAL_ERROR: SSL_ASSERT failure in ../mpc/clean.C @ 372 - elemP
%ECPA-0-MSG: slot3 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```
These are cosmetic changes to the error message that is displayed when no LUs are available, so there is no bug to workaround. The following message is currently displayed on the router console when a client attempts connection to a generic LU and none is available:

%CIP2-4-MSG: slot4 %TN3270S-4-NO_LU_SESSIONS: No LU sessions left in :GENERIC for PUs at IP addr 172.18.5.202, port 23

This message will be enhanced to give an indication of the client that attempted to connect. The modified message shall be as follows:

%CIP-4-MSG: slot4 %TN3270S-4-NO_LU_SESSIONS: Client session 10.83.120.43:1195 requested a generic LU from IP 172.18.5.202:23, but no LU is available.

Additionally, if 10 such connect attempts are made from the same client, the client will be put into a hold state and the following message will appear on the client screen:

THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.

There is no workaround. [CSCds33140]

- The fatal error 35 occurred in cip27-5 and above when the command no pu puName was executed. This occurs only when one of the logical units (LUs) is in a hold state and this command is executed. This fix will help in preventing the crash from happening.

There is no workaround. [CSCds39875]

- The CIP card configured for Cisco Multipath Channel (CMPC) hangs with the following messages:

%RSP-3-RESTART: interface Channel0/2, output stuck
%LINEPROTO-5-UPDOWN: Line protocol on Interface Channel0/2, changed state to down

The problem can also be seen by performing a “tasks” command on the CIP console where the central processing unit (CPU) is at 100 percent. Both symptoms are triggered by adding new Cisco Multipath Channel Transmission Groups (CMPC TGs) or the flapping of existing TG(s).

A potential workaround is to add new TG(s) only during a maintenance window and update the configuration immediately following a reload of the microcode. [CSCds41393]

- When a client disconnects, and the server is configured for lu termination termself, the server always sends the inbound TERMSELF, byte 3, as 0x44 indicating forced termination. To avoid operator intervention upon a subsequent connect, this should be sent inbound as 0x4C, indicating cleanup. Similarly, when configured for lu termination unbind, the UNBIND always flows inbound with byte 1 = 0xFE, indicating session failure. This should be 0x0F, indicating cleanup.

There is no workaround. [CSCds44696]

- The CIP/CPA restarts with a fatal error 35 when a transmission group (TG) is configured with an adapter number that exceeds the limit of 18. This occurs at all CIP/CPA code levels.

The workaround is not to exceed the limit of total number of adapters that can be associated with all TGs, that is, 18. [CSCds47000]

- A fatal error 32 can occur when deleting a transmission group (TG) for Cisco Multipath Channel Plus (CMPC+) and then reconfiguring it.

There is no workaround. [CSCds48048]

- The TN3270 server translates systems network architecture (SNA) type commands to their non-SNA version before being sent to the TN3270 client. For example:

0xF5 is translated to 0x05
0xF1 is translated to 0x01
and so on.
This DDTS request is for a command to allow users not to have this translation occur. So, when configured properly, the SNA version of the TN3270 commands would flow through to the client unmodified.

There is no workaround. The TN3270 server always translates the commands. [CSCd48150]

- The TN3270 server is configured with both static and dynamically created logical units (LUs). Physical units (PUs) are created under listen points. The following fatal error 35 message occurs in the TN3270 Response Time Work Thread:

  %CIP2-0-MSG: slot1 %ACCOUNT-0-FATAL_ERROR: Fatal error (code=35)

  There is no workaround. [CSCd49209]

- The TN3270 client configured for VT100 ANSI terminal should not be able to negotiate a session with the TN3270 server. This terminal type will be added to the list of unsupported terminal types. There is no workaround. [CSCd51099]

- The TN3270 clients that are nailed to dynamic Logical Units (LUs) might be unable to reconnect once the LUs are placed on the TN3270 server bad queue. This could happen if the LU has been inactivated (Deactivate Logical Unit, or DACTLU) when the client previously connected. The server mistakenly might think the LU has been varied inactive (via Virtual Telecommunications Access Method, or VTAM), and will not allow subsequent reconnection to the LU.

  The workaround is once the LU is in this state (on the bad queue and the server will not allow reconnection), the only recovery is shut/no-shut on the PU, or to vary the PU as inactive/active. To avoid this situation, one might code **lu deletion never**, so that DACTLU does not flow when a client disconnects from the LU. [CSCd67701]

- A fatal error 35 occurs when forcing the Multiple Virtual Storage (MVS) of a Primary Dependent Logical Unit Server to stop by the **QUIESCE** command. This problem is seen at any time with the **QUIESCE** command.

  There is no workaround. [CSCd72088]

- A fatal error 35 might occur if the client is in the “hold state” and attempts to reconnect to the same resource. A client enters the hold state after attempting to connect to an invalid resource or one which is not currently available 10 consecutive times. Normally, if a client attempts to connect to the same resource again, he would just get the “hold state” message. As a result of this bug, a fatal error 35 might occur instead. This problem occurs as a result of the resolution for CSCdr50532, so therefore only exists in Release 27-12.

  The workaround when the client is in the “hold state” is to attempt to reconnect to a different resource rather than attempting to reconnect to the same resource. [CSCd92038]

**Microcode Release 27 Caveats**

This section describes the open and resolved caveats for microcode release cip27 and xcpa27. The caveats listed apply to only the most serious problems.

**Open Caveats in Version 27.35/Resolved Caveats in Version 27.36**

This section describes possible unexpected behavior in Version 27.35. All the caveats listed in this section are resolved in Version 27.36.

- CIP/xCPA CLAW packing trace entries do not show sufficient information to diagnose activation problems. This occurs under all conditions.
There is no workaround. [CSCsd96288]

- The CIP/xCPA CLAW packed activation fails under unknown conditions. There is no workaround. [CSCsd96278]

- A Cisco CMCC configured for CMPC LLC might fail due to a buffer shortage. This might occur when the local major node for one side of the connection is inactive while the other side is attempting to connect. The workaround is to configure the link to use the CSNA feature rather than CMPC. [CSCse91888]

- A VTAM USSMSG that is too large to fit on a 24x80 screen might cause the CMCC tn3270 server to fail. A VTAM USSTAB entry used by the TN3270 clients was configured incorrectly, as explained in IBM APAR II12568. The workaround is to modify the USSTAB so that it fits on a 24x80 screen. Please correct the misconfigured VTAM USSTAB entry per IBM recommendations in APAR III12568. [CSCsf26598]

### Open Caveats in Version 27.34/Resolved Caveats in Version 27.35

The open caveats that were to be in Version 27.35 were incorporated with those in the release of Version 27.36, because Version 27.35 was not released.

- The CIP console commands **tn3270 resources**, **tn3270 scan**, and **tn3270 stats** may produce incorrect output because multiple commands are issued very quickly, for example, by pasting in multiple commands. The workaround is to allow the previous command to complete displaying its output before entering a new command. [CSCsc79152]

### Open Caveats in Version 27.33/Resolved Caveats in Version 27.34

This section describes possible unexpected behavior in Version 27.33. All the caveats listed in this section are resolved in Version 27.34.

- Customers unable to access target applications via CIP Tn3270. Tn3270 Capture Trace indicates that NO PUs are available for usage, as shown here:

```plaintext
Aug 3 11:40:44.371 EDT: %CIP2: slot0 [bad telnet connect]13[lpAddrClient]10.128.69.147:[tcpPortCl
Aug 3 11:40:44.371 EDT: %CIP2: slot0
-----ient]0x891:[connectReasonCode]0x8:[tn3270eDeviceType]IBM
Aug 3 11:40:44.371 EDT: %CIP2: slot0
-----3279-2-E:[tn3270eDeviceName]:[tn3270eSubErr]no pu:
```

This issue is seen when the CIP card is low in memory. See the following example from the **show controller cbus** command:

```plaintext
... Load metrics: Memory dram 1794472/32M ...
```

The workaround is to ensure that memory installed on the CIP card can handle the current workload. A microcode reload or an OIR on the affected CIP card that is running low in memory can be used to recover the memory on the affected CIP card. [CSCsb70794]

- TN3270 clients cannot connect to CIP/ECPA TN3270-server listen-point after a change is made to the number of the clusters in a pool under a PU. This occurs when the change is made when the number of clusters allocated to the pool in the PU is at the limit on LUs. Specifically, if the pool as at the limit and the following is issued:
no allocate lu 1 pool TEST clusters 5  
allocate lu 1 pool TEST clusters 5

Then clients may fail to connect. This affects both LUs in the TEST pool as well as the LUs remaining in the generic pool (unassigned LUs).

The workaround is to reactivate the affected PUs. This can be accomplished either by a VTAM VARY INACT/ACT or by a shutdown | no shutdown of the PUs. [CSCei70033]

**Open Caveats in Version 27.32/Resolved Caveats in Version 27.33**

This section describes possible unexpected behavior in Version 27.32. All the caveats listed in this section are resolved in Version 27.33.

- CIP/CPA LLC sessions disconnect with FRMR. This occurs when a customer runs a very heavy traffic load on the CIP/CPA and retransmissions occur.
  
  There is no workaround. [CSCeh75068]

**Open Caveats in Version 27.31/Resolved Caveats in Version 27.32**

This section describes possible unexpected behavior in Version 27.31. All the caveats listed in this section are resolved in Version 27.32.

- It might not be possible to reactivate a tn3270 server PU after it has been inactivated on the mainframe. The mainframe may log the following type of messages: IST680I CONNECTION REQUEST DENIED-ID=puname PU GEN NOT SUPPORTED IST1394I CPNAME=NETID.puname STATION ID=020011101255 IST081I LINE NAME=L064001D, LINE GROUP=XCACIP0G, MAJNOD=XCACIP00 .
  
  The CIP may log the following type of messages: %ECPA4-6-MSG:slot1 %MSG802-6-LLC_DUP_CCB: LLC Station : RMAC=4000 .7507.0001 LMAC=4000.7507.0001 LSAP=04 RSAP=0C
  
  The workaround is to configure the tn3270 server PU as "shut" then "no shut". [CSCeg46357]

- The following message may be seen from a CMCC adapter when very many tn3270 PUs are configured: %ECPA4-6-MSG:slot2 %MSG802-6-LLC_DUP_CCB: LLC Station : RMAC=4043.3333.9000 LMAC=4041.2222.001F LSAP=08 RSAP=88.
  
  There is no workaround. [CSCeg74214]

- When the CMPC+ connection is activated, the following message may be seen: %CIP2-3-MSG: slot1 %MPC-3-CMPCP_CV_ERR1: Unrecognized/Unexpected CV: 040C.
  
  The problem was reported after the mainframe operating system was upgraded to z/OS R1.5. The control vector 040C contains a list of supported functions and was added for IPV6 support on the mainframe.
  
  The CV is ignored on the CIP.
  
  There is no workaround. [CSCeg84750]

- Under a very heavy load, a Cisco Channel Interface Processor, CIP2, or Channel Port Adapter, ECPA or ECPA4, might unexpected disconnect an LLC2 session. The problem only occurs when LLC2 dynamic windowing, llc2 nw N, is configured and an LLC2 REJ frame is received.
  
  The workaround is to remove the llc2 nw N command. [CSCeh50081]

- The CIP/xCPA llc badns command is erroneously reporting LLC sessions that did not experience the badns condition. This causes one to believe a certain LLC session had a problem when in fact it did not. If an llc session experiences the badns condition, subsequently disconnects and the control block representing that session are reused. The new LLC session will show as having experienced a badns condition in the output of the CIP/xCPA llc badns command.
  
  There is no workaround. [CSCeh51794]
Open Caveats in Version 27.30/Resolved Caveats in Version 27.31

This section describes possible unexpected behavior in Version 27.30. All the caveats listed in this section are resolved in Version 27.31.

- The Channel Interface Processor (CIP) running microcode cip27-29 crashes with Fatal Error (code=35) if the following command is entered without specifying a logical unit name: `% `tn3270 stats lu`. The failure only occurs if a logical unit name is not entered.
  The workaround is to specify a logical unit name as a parameter of the command. [CSCeg31452]

- When shutting down the TN3270 server a fatal error 35 may be experienced. This occurs after failure of a DLUR link.
  There is no workaround.[CSCdz27554]

Open Caveats in Version 27.29/Resolved Caveats in Version 27.30

This section describes possible unexpected behavior in Version 27.29. All the caveats listed in this section are resolved in Version 27.30.

- The TN3270-server sends up many Signal Request-to-Send (RTS) RUs to VTAM causing a VTAM hot I/O condition. A client generated many IAC Breaks (or IAC IPs - Interrupt Process) which the TN3270-server converted into Signal Request-to-Send (RTS) RUs. At the same time the CIP/xCPA sent LSA flow_off to VTAM preventing it from sending the Signal +RSPs back to the TN3270-server. This caused the VTAM IOBUF pool to be exhausted.
  Workaround: Specifying MAXSLOW=15-30 (seconds) in the VTAM XCA major node will cause VTAM to terminate the PU if it remains in this flow off condition more than the time period. This will prevent the excessive IO from impacting VTAM. This only applies when the PU connects to VTAM via an XCA major node. [CSCef08617]

- A 7206vxr router with a PA-4C-E XCPA Port Adapter may incur a Fatal Error 35 Error code causing the XCPA adapter to reload. The IOS being run at the time was 12.2(10b) with XCPA microcode level 28-11.
  There is no workaround. [CSCef05612]

- The following CMCC messages might be observed when TN3270 services stopped and started. The messages are: CMCC-4-CFGFAIL and CMCC-3-CFGCMDDROPPED: Config queue is full, command was dropped. The problem happens if there are more than 1800 Tn3270 Dlur PUs configured under virtual channel interface.
  The workaround is to reduce the size of the Tn3270 PU configuration. Distribute Tn3270 PU configurations to different CIP routers. [CSCee89157]

- The following message may be displayed on a client screen: THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM. Printers may print garbage characters. This occurs when a client IP has had 10 consecutive connect failures. This “feature” was added to prevent the CIP from wasting resources on answering TN3270 client which is asking for an unavailable VTAM resource. There have been problems with this operation with printer servers where multiple printers may appear as the same client IP address. The customer requests a way to disable this feature.
  There is no workaround. [CSCdr32459]
The following messages are observed on a CIP/xCPA when attempting to configure a new TN3270-server PU: 3d00h: ECPA41-InsertPuIntoResourceTree: avl_insert failed for O41C0001. 3d00h: %CMCC-4-CFGFAIL: Interface Channel1/0: configuration command TN3270S_PU_NEW cmd 16 failed. This can occur when adding PUs with the following characteristics:
- The first 6 characters are the same as other PUs already defined
- The PUs are not specifying the luseed parameter
- PUs have statically defined LU names matching the 1st 6 characters of previously defined PUs.
Workaround: Ensure that the luseed parameters used on all PUs are unique. [CSCef70598]

Cisco SNA (CSNA) responds to a TEST frame with a DISC frame even if we inactivate an External Communications Adapter (ECA) major node from a Virtual Telecommunications Access Method (VTAM). It should be ignored.
There is no workaround. [CSCef66551]

The channel interface processor got the fatal error 37 after the channel interface shut down to recover OSPF routes. CONFIG-3-WORKLEFT: Work pending on work queue when device terminated.
There is no workaround. [CSCef28648]

Open Caveats in Version 27.28/Resolved Caveats in Version 27.29

This section describes possible unexpected behavior in Version 27.28. All the caveats listed in this section are resolved in Version 27.29.

- A fatal error 35 may occur when a PU with LU pools already present. This problem will occur if any of the LUs (associated with the new PU) have the same name as the previously added LU pool. LU names are created based on the first six characters of the PU name and appending a 2 digit (hex) locaddr. If this results in a name which is the same as an LU pool name, then this fatal error 35 will occur.

To work around this problem, do not define pool names and PU names which are the same in the first six characters. If the pool and PU names happen to be the same in the first 6 characters, then lu-seed should be used on the PU definition so that the LU names created won't be the same as any pool name. [CSCee32607]

- This fatal error occurs: %XCPA-3-STATUS: bay [x] Fatal error detected (code=35)
  %ECPA4-0-MSG: slotx %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

Immediately following a NO SHUT on the channel interface, the ECPA4 encountered a fatal error and dumped.
There is no workaround at this time. [CSCee40253]

Open Caveats in Version 27.27/Resolved Caveats in Version 27.28

This section describes possible unexpected behavior in Version 27.27. All the caveats listed in this section are resolved in Version 27.28.

- If a c7000 has a CIP card configured with many tn3270 server PUs, when the channel x/2 interface is shut down to allow a backup CIP to take over operation), IOS may issue the following message:

  %CIP2-3-MSG: slot0 %MSG802-3-HARD_ERROR: cls_cip_term: Cleanup takes too long-force takedown

The workaround is to issue a "microcode reload" to ensure that the CIP ucode integrity is restored. [CSCee03080]
A Cisco Mainframe Channel Connection (CMCC) configured for CSNA might reload with a Fatal Error 35 if the connected mainframe stops responding. These conditions are necessary to see the problem: The CMCC is configured for CSNA. The virtual interface is started then shutdown. The connected mainframe stops responding without shutting down the CSNA device. [CSCee03619]

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 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.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and 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. [CSCee35335]

Open Caveats in Version 27.26/Resolved Caveats in Version 27.27

This section describes possible unexpected behavior in Version 27.26. All the caveats listed in this section are resolved in Version 27.27.

- The Tn3270 PUs are in a WAIT state. The Virtual Channel Interface is in a Down/Down condition.
  Messages seen in the log:
  TN3270S-0-ILLEGAL_CCMUTEX_RELEASE: CIP2 slot1 : Releasing unacquired semaphore, lock_held 800A9C4C lock_value FFFFFFFF ccMutex tcb 8010FCDO thread tcb 81459CB0
  The Tn3270 PUs were hung and the Customer Shut/No Shut the Virtual Channel interface in an attempt to recover. The PUs would not recover.
  The workaround is to reload the CIP Microcode.

- In a Cisco 7500 router with a CIP2, the CIP2 may crash with a fatal error 32. The problem also may occur on a Cisco 7200 with an XCPA.
  The problem may occur when a channel interface with CSNA(s) is shutdown or when a CSNA is unconfigured.
  There is no workaround.

- CIP/XCPA TN3270 Server converts USSSCLS USSMSGs to 3270 datastreams for TN3270E clients even if they have negotiated the SYSREQ function.
  The TN3270 client must negotiate TN3270E and the SYSREQ function without negotiating the BIND-IMAGE function.
  There is no workaround.
Caveats for CIP and CPA Microcode

- The CIP microcode unexpectedly reloads with fatal error 35.
  This is a rare occurrence that can happen if a tn3270 client is disconnected during the processing of data to that client.
  There is no workaround.
- CIP2-6-MSG: slotx %ADAPTER-6-LOGOUT: ESCON dump output is followed by the
  %DEBUGGER-0-FATAL_ERROR: Fatal error (code=37) dump.
  The write subchannel receives a HSCH or a CSCH while the read subchannel is waiting for access to the channel. This will only occur with very heavily utilized claw packing channels.
  This was observed with a feature of a mainframe TCP/IP stack that stopped and restarted a packed CLAW connection. The stack restarted the CLAW connection when there was no input from the CMCC.
  The workaround is to avoid stopping packed CLAW links while there is traffic.
- PU activation is intermittent. Sense Code 10160004 will occur. The PU will eventually activate.
  Running CIP28.14 and TN3270 configured with PUs defined
  There is no workaround.
- The message: SCB limit on port NN reached, correlator: NNNN task: NAME XXXXXXXXX. might
  be seen for a Channel interface, CIP2 or XCPA.
  Many CSNA definitions are removed or shutdown.
  The workaround is to reload the microcode on the interface.

Open Caveats in Version 27.25/Resolved Caveats in Version 27.26

This section describes possible unexpected behavior in Version 27.25. All the caveats listed in this section are resolved in Version 27.26.

- If you configure the router for CLAW packing but do not change the TCPIP profile, then the following message might be seen:
  Mar 17 07:49:18 EST: %CIP2-6-MSG: slot0 %PACK-6-RANGE2: Out of range sublink (64) received in packed claw message.
  Prior to CIP and CPA microcode version 28.14, the error message does not identify the host that is sending the invalid frames. There is no workaround.
  With microcode version 28.14, the CLAW packing error messages include the path and device address to identify the connection on which the error is being generated. [CSCea52705]
- A TN3270 client will not receive the VTAM USSMSG10 screen or get a LOGAPPL session when its current LU-LU session ends if the DLUR/DLUS connection has failed and restarted during the active LU-LU session.
  This problem will only occur on TN3270 clients that are actively in session when/if a Backup DLUS takes over.
  There is no work around. If the client disconnects from the LU and reconnects it will get a USSMSG10 or LOGAPPL session. [CSCec04176]
- Router started getting %ADAPTER-6-LOGDATA error then the CIP crashed with a Fatal Error 37. [CSCec07315]
- tn3270 clients are slow or are failing to connect to the tn3270 server in CIP/CPA when Tn3270 is configured on CIP/CPA.
The workaround is to identify the client that is requesting a large number of sessions, is not completing the three-way handshake and is using an ACL to filter. A temporary workaround would be to shut and no shut the Tn3270 or a specific PU identified as the clients destination IP address. [CSCec16766]

- CIP/xCPA TN3270-server PUs go into ACT/BUSY state for extended periods of time. Eventually the PUs recover and return to ACTIVE state without any intervention.

  The PUs go into ACT/BUSY state when the upstream LLC2 link enters local busy state. This is due to TN3270-server keeping buffers that it received from LLC2 until the client acknowledges them with a TCP level ACK.

  This occurs with both TN3270-server DLUR PUs and direct PUs.

  There is no workaround [CSCec57475].

- TN3270-server will allocate an LU to a TN3270 client even if the LU has never been unbound from VTAM. This can lead to session setup failures with sense code 0805000B - Session limit exceeded.

  This is known to occur when TN3270-server is configured with:

  - DLUR
  - LU termination termself
  - LU deletion never - This is the default
  - Multiple upstream links
  - Application that the LU is in session with is not on the DLUS host
  - RESETLU=NO is coded on LU or LUGROUP definition in VTAM

  It also can happen for any reason where the DLUS host cannot/does not notify the application host of the termself.

  Workaround: In the another scenario, specifying RESETLU=YES causes VTAM to DACTLU/ACTLU the LU and notify the application host to send the UNBIND. This will prevent the problem. [CSCec58447]

- XCPA/CIP experiences a Fatal Error 35

  A TN3270 server PU configured with all dynamic LUs can put the TN server in a loop. When the client is trying to connect to the dynamic LU for the very first time, the LuCb is not yet created, and this was putting the server in the loop.

  In the customer’s environment, they had dynamic LUs configured under all the PUs. And after they brought up the tn3270 server, after a microcode reload, the client tried connecting to those LUs.

  There is no known workaround. [CSCec59077]

- TN3270-server DLUR controlled LU logon fails with either sense 80140003 or 087D0001. Topology on DLUS shows an ENDPT TG as OPER when in fact it is no longer operational.

  CIP/xCPA TN3270-server DLUR with multiple end point transmission groups (TGs). TN’s DLUR name (CP name) must be greater in the collating sequence than the CP name of the DLUS.

  Workaround: Determine the TG that is really not operational but is listed as operational on the DLUS host and delete it. [CSCec70608]

Open Caveats in Version 27.24/Resolved Caveats in Version 27.25

This section describes possible unexpected behavior in Version 27.24. All the caveats listed in this section are resolved in Version 27.25.
• A deactivate LU (DACTLU) operation on an LU in the middle of a multi-LU cluster pool could render the entire cluster unusable. The same is true if the statically defined LU is not available on the host, but is configured on the router in the middle of a cluster. When this occurs, the client is not granted connection beyond the faulty LU.

There is no workaround. [CSCdr95560]

• The output from the `show extended channel tn3270-server dlur` command shows the CP-CP status as NOTKNOWN.

This problem occurs if there is more than one DLUR-DLUS link to the Network Node Server (NNS) and the CP-CP session is not on the first link in the router configuration.

There is no workaround. [CSCdx39152]

• When we inactivate an XCA major node in VTAM, VTAM has sent DACTPU commands and received DACTPU ACKs to/from all of the TN3270 server PUs. However, some TN3270 server PUs may not become inactive and subsequently cannot be activated. When this occurs, the TN3270 server PU status (shown using the `show extended channel tn3270-server` command) remains as “P-ACTPU” or “ACT-BUSY”.

The workaround is to run the `shut` and `noshut` commands at the PU scope, which properly activates any PUs that are suspended in this condition. [CSCe47302]

• If a CMPC connection from an OS host is inactivated by VTAM (the local major node PU is inactivated), then the router log reports the following message:

  CIP2-3-MSG: slot5 %MPC-3-BAD_HDR: Unrecognized MPC header received: 0000C000 00000000

  The CIP does not clear the LLC2 connection. Therefore, the upstream link remains connected.
  CMPC is not processing the DISCONTACT request from VTAM, so the LLCC (MPC LLC) connection is left in a bad state preventing the subsequent attempts to activate the LLC connection from completing.

  This problem does not exist between the CIP and OS/390 systems.
  The workaround is to reconfigure the connection using CSNA or CMPC+. [CSCe71612]

### Open Caveats in Version 27.23/Resolved Caveats in Version 27.24

This section describes possible unexpected behavior in Version 27.23. All the caveats listed in this section are resolved in Version 27.24.

• Print jobs through an Open Connect print server are sometimes suspending.

  This is occurring when the host application fails to send an End Bracket Indication (EBI) to the Secondary Logical Unit (SLU, which is the printer) prior to unbinding the session. The EBI triggers the TN3270 server to send IAC-Abort Output (AO) to the client that indicates the print job is complete. In the absence of EBI, the IAC-AO is not sent to the printer, and the print does not complete.

  With the fix, the CMCC TN3270 server sends AO (Abort Output) to non-E printers or End of Job (EOJ) for E-printers when it is in receive state (in bracket in the outbound direction) when the TN3270 server receives an UNBIND. This will force data previously written to the printer to be printed.

  There is no workaround. [CSCdp72090]

• The number of LUs in the output from the `show extended channel tn3270-server` command varies when nailing is configured on the CIP or CPA.
This example sets up 5 LUs in the host. The TN3270 server is configured on the CPA without nailing. The output from the `show extended channel tn3270-server` command shows 10 LUs:

```
Router# sh extended cha 4/0 tn
```

```
server-ip:tcp          <current stats> < connection stats > <response time(ms)>
          lu     in-use     connect     disconn     fail     host     tcp
10.0.0.23:23         10          0            0           0          0     0
```

However, when you configure nailing, the output from the `show extended channel tn3270-server` command shows 5 LUs:

```
Router# sh extended cha 4/0 tn
```

```
server-ip:tcp          <current stats> < connection stats > <response time(ms)>
          lu     in-use     connect     disconn     fail     host     tcp
10.0.0.23:23          5           0            0           0          0     0
```

There is no workaround. [CSCdx93118]

- When using the NetSolve application on the mainframe to query the CIP for TN3270 LU names, you might see the LU name display as a blank or the LU name might be incomplete.

  The problem is only seen on applications that use the TN3270 Monitor interface to the CMCC TN3270 server.

  The workaround is to use the Cisco IOS `show extended channel tn3270-server` command to display LUs. [CSCdz15898]

- CCA-0-DEV_ERR2: Device error but no active defined device.

  The CIP or CPA crashes with DEBUGGER-0-FATAL_ERROR, unexpected reload with fatal error code=37. The CIP or CPA receives a frame from the host mainframe, but due to a logic error in the ESCON chipset on the CIP and CPA, it is not handled correctly. The CIP or CPA detects the logic error in the chipset and forces a microcode reload with a fatal error.

  There is no workaround. [CSCdz31806]

- The output from the `show extended channel tn3270-server pu` command displays the LU as inactive while the VTAM display from the command `d net,id=nnnnnnn,e` (where `nnnnnnn` is the LU name) shows the LU as unstable.

  The client connects to the TN3270 server and TN3270 sends a Notify Available to VTAM. If the client disconnects while TN3270 is still waiting for the Notify response, and if the response is not received in a predefined timeout, the described symptom can occur. This is because TN3270 puts the LU in reset state without notifying VTAM. TN3270 now has the LU as being inactive while VTAM thinks it is active, but unstable. An attempt to inact/act the LU at this point results in the LU being stuck in the PDACL state in VTAM.

  There is no workaround. [CSCdz36410]

- A fatal error 35 might occur on the CIP or CPA when you issue a command from within the TN3270 server configuration prompt.

  The fatal error 35 is observed when the `no listen-point` command is issued as shown in the following example, where `xxx.xxx.xxx.xxx` is the IP address of the listening point:

  `no listen-point xxx.xxx.xxx.xxx`

  There is no workaround. [CSCdz38654]

- The CIP TN3270 server advertises its MAX I-FIELD=4105 during XID negotiation even though the RIF indicates the MAX frame is 1500 bytes.
When sending an XID, the value being reported for the maxIField (bytes 10-11 in XID) might be too large if the previously received RIF from a test packet indicates a lower value. The TN3270 server should be comparing its MaxIField from the SAP with the MaxDataRoute (received from the link-station partner via Test/RIF), and report the smaller of the two when sending the XID.

There is no workaround. [CSCdz38697]

- Under certain circumstances when the TN3270 server is configured for DLUR, it can misinterpret the SLU name it receives if the PCID includes x4B in the received bind request. The LU-LU session is unbound with sense code 8004 0000.

In this situation, the TN3270 server is configured as DLUR. The DLUS returns the SLU name not network qualified. The PCID contains x4B.

There is no workaround. [CSCdz48129]

- The status of the LU in VTAM is PSESEND-P, while the LU state on the router is ACT/NA.

This problem can occur if a client is bound to an application, but has entered the SSCP session (via system request key) to make a request. In this case, the TN3270 server thinks that the client is waiting to be bound to some other application. If the client disconnects while in this state, the server goes into a “waiting for bind” condition and ignores a subsequent unbind (because the server incorrectly thinks that the LU is not currently bound). When VTAM receives no response to the unbind, the LU is placed into the PSESEND state.

There is no workaround. Once the condition is observed, you must cycle the LUs in VTAM. [CSCdz69040]

- When a client connects to an LU, the LU will sometimes suspend in a P_NTF/UA state as shown in the following sample output from the show extended channel tn3270-server pu command:

  Router# sh ext chan 5/2 tn3270-ser pu PUNAME

<table>
<thead>
<tr>
<th>lu</th>
<th>name</th>
<th>client-ip:tcp</th>
<th>nail</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>RA5V0202</td>
<td>10.61.4.102:44291</td>
<td>N</td>
<td>ACT/SESS</td>
</tr>
<tr>
<td>3</td>
<td>RA5V0203</td>
<td>10.43.8.86:2642</td>
<td>N</td>
<td>P-NTF/UA</td>
</tr>
</tbody>
</table>

This problem is the result of a small timing window when a client connects to an LU (logical unit) before that LU session has completed the cleanup from a previous client connection.

The workaround is to deactivate the LU at the host and reactivate it. [CSCdz75177]

Open Caveats in Version 27.22/Resolved Caveats in Version 27.23

This section describes possible unexpected behavior in Version 27.22. All the caveats listed in this section are resolved in Version 27.23.

- The CIP does not clean up properly after VTAM or an XCA major node is recycled. The following error messages appear in the router log:

  %ECPA-6-MSG: slot1 %MSG802-6-LLC_DUP_CCB: LLC Station :
  RMAC=4000.4000.0002 LMAC=4000.4000.2222 LSAP=04 RSAP=C6

  6:43:13.323: %ECDA-6-MSG: slot1 %MSG802-6-CHP_DUP_CCB: CH_Port:
  RMAC=4000.4000.0002 LMAC=4000.4000.2222 LSAP=04 RSAP=C6

  6:43:13.323: %ECDA-6-MSG: slot1 %MSG802-6-CHP_DUP_CCB: CH_Port:
  RMAC=4000.4000.0002 LMAC=4000.4000.2222 LSAP=04 RSAP=C6

  Note: The following workaround might lead to a CIP microcode reload, and should only be performed if a CIP microcode reload is a tolerable side effect.
The workaround is to issue the `shut` command followed by the `no shut` command while in TN3270 PU configuration mode. This seems to clear the PU condition, and the PU goes to active status. [CSCdr90542]

- TCP connections for TN3270 clients might remain in the close-wait state indefinitely after a client disconnects.

This problem only occurs if the client happens to disconnect while the LU (logical unit) is in the state of waiting for ACTLU (activate LU). This might occur if the LU group major node is not active, or if ACTLU is slow to arrive. If the client reconnects, a new TCP connection would be opened while the old connection remains in close-wait. The new connection will operate normally.

There is no workaround. [CSCdx01730]

- A NO_BIND_REQ_RCVD error is logged for TN3270 printers and the printers disconnect.

When a printer connects to the TN3270 server, but no print jobs are ready to be printed, the TN3270 server disconnects after 2.5 minutes and a NO_BIND_REQ_RCVD error is logged. If this occurs, subsequent printing fails because the printer is no longer connected.

The TN3270 server should not disconnect printers when a BIND is not received within 2.5 minutes. This should only occur for LU type 2 (display) clients.

The workaround is to verify whether print jobs are ready to be sent to the printer before connecting to the TN3270 server. [CSCdx58390]

- Performance improvements for the CIP and CPA.

You might see any number of symptoms that might be impacting overall system performance. First, you might see many RDBs (Read Dropped Blocks) as shown in the output from the `show extended channel statistics` command. In the following example, `xxx` is the number of read dropped blocks caused by a temporary (normal) condition of no memory buffers available for queueing to the mainframe:

```
Router# show extended channel 1/0 statistics
Path: 0150 -- ESTABLISHED

<table>
<thead>
<tr>
<th>Command</th>
<th>Selective</th>
<th>System</th>
<th>Device</th>
<th>CU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dev</td>
<td>Connects</td>
<td>Retries</td>
<td>Cancels</td>
<td>Reset</td>
</tr>
<tr>
<td>D0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Blocks</td>
<td>Bytes</td>
<td>Dropped Blk</td>
<td>Memd</td>
<td></td>
</tr>
<tr>
<td>Dev-Lnk</td>
<td>Read</td>
<td>Write</td>
<td>Read</td>
<td>Write</td>
</tr>
<tr>
<td>D0-00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

This particular condition has been aggravated by the addition of the Gigabit Ethernet NIC feeding the CIP as an ingress network port. Additional symptoms might be noticed by a large amount of overhead in the CMPC Plus channel IO packets sent to the mainframe.

**Note**

CMPC Plus users should refer to IBM APAR/PTF PQ61503/AQ61503 prior to installing this level of microcode (or subsequent levels of microcode). Refer to this APAR to find the appropriate sysrouted APAR for your OS release due to data corruption issues found on the IBM mainframe.

There is no workaround. [CSCdx72717]
- The CIP or CPA interfaces that are configured for CLAW can get fatal error 37. The fatal error 37 can appear after the following messages:

```
%%%BSQ-0-SCB_CHAIN: CIP2 slot4 : Read SCB chain is out of sequence
```

or

```
%%%ADAPTER-6-LOGOUT: CIP2 slotX : Port N logout data. Adapter microcode C50602D4
```

The mainframe syslogs will show channel errors for the devices. The fix allows for additional error checking conditions so the ESCON code can recover and not take a fatal error.

There is no workaround. [CSCdy06181]

- A CIP running TN3270 might experience memory leaks in the TN3270 response time task, which eventually takes down the CIP with a fatal error 37:

```
%CIP2-3-MSG: slot1 %CBUS_ATTN-3-DUMPUCODE: Dump of the CIP microcode has been requested
%CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=37)
```

There is no workaround. [CSCdy10459]

- The CIP or CPA might crash with a fatal error 35 in Aluc_Start_SscpLu. This is a very rare occurrence due to a small timing window when a client might disconnect while some other event (host packet processing) is in progress. This could incorrectly leave the LU (logical unit) in the LU-LU session state, even though the client has disconnected. The result is that upon receiving subsequent packets (such as BIND, UNBIND), the server attempts to reference data structures that have been freed, resulting in the fatal error.

There is no workaround. [CSCdy20175]

- Unused Cisco Multipath Channel Transmission Group (CMPC TG) connections might lead to a buffer shortage in the CIP or CPA. The result is that no CMPC TGs will be able to reconnect once disconnected. This has been observed on a CPA running xcpa26-26 microcode.

The workaround is to disable the host PUs (physical units) associated with the CMPC TG to stop the buffer leak root cause, and then to issue a microcode reload to recover the lost buffers. Another workaround is to remove any unused CMPC TGs from the router configuration. [CSCdy44696]

- LLC_DUP_SAP, fatal error 9 in ssi_buff.c, or PUs in P-ACTPU state due to a buffer loss condition. It’s possible that other errors (such as ACT/BUSY on PUs) could occur as a result of this buffer loss.

The TN3270 buffers that are used to communicate to LLC layer are being lost, which eventually results in a depletion of the buffers and can cause any of the errors mentioned above. This buffer loss can occur during a link close or disconnect operation, such as would occur during a “shut” of TN3270, a listen-point or PU. A buffer is lost for each PU doing the close or disconnect operation.

The buffer pool that is getting depleted is shown in the “tn3270 stats” (in the CIP or CPA console). The second line from the bottom of the stats output, is referred to as the “DLUR inbound pool free buffers.” The title is misleading as these buffers are also used for direct PUs...

The following example shows the normal number of free buffers (150) in the DLUR inbound pool. When this buffer pool is low or depleted, the problems mentioned above can occur:

```plaintext
[snip]
LStn Svcs inbound pool free buffers 520
DLUR inbound pool free buffers 150 <=====
DLUR outbound pool free buffers 520
```

There is no workaround. [CSCdy46286]
• The CIP Dumps with a fatal error 35 in RcvDACTxU.
A DACTLU (deactivate LU) packet is being received to an LU (logical unit) which the DLUR application does not currently have defined. DLUR should be rejecting the DACTLU with sense 08120007 rather than crashing with a fatal error.

There is no workaround. [CSCdy85034]

Open Caveats in Version 27.21/Resolved Caveats in Version 27.22

This section describes possible unexpected behavior in Version 27.21. All the caveats listed in this section are resolved in Version 27.22.

• The CIP crashes with a fatal error code 35. Just before the crash, the following type of error is logged:

```
bad LU on DISC: PU index is -1, LOCADDR is 216, DISC reason is 19
..remote IP address = 80.1.25.67, tnetSession = EE33BEAF, ipNext=0
%TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]:
:216 pu:FF55DEAD, tnet:EE33BEAF
%TN3270S-1-LU_ERROR_INFO: LU info: Event 9 10 10 16 12 10 4
8 9 10 10 16 17 1 15
```

This error occurs after doing a “shut” on the TN3270 server. This could occur anytime the server attempts to disconnect an LU but the PU is in the process of being deleted.

There is no workaround. [CSCdr11739]

• If the TN3270 server rejects the Activate Logical Unit (ACTLU) with a 08970000 sense code, the LU is not properly placed in the INACTIVE state on the server (VTAM thinks the LU is inactive and the server thinks it is active). This confusion appears in the ‘show’ outputs. In future connect attempts to the LU, the server waits for LU-LU responses from the VTAM which it will not get since there is no LU-LU session. The server logs messages such as NO_BIND_REQ_RCVD and NO_NTFY_AV_RSP_RCVD.

There is no workaround. [CSCdu40765]

• After a TN3270 client disconnects, and while the disconnect processing is occurring, an inactivity timer expires on the client, forcing the TN3270 server to try to disconnect the client that is already disconnected. The following message occurs:

```
%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]: luname:72
pu:80F1A2A0, tnet:0
%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR_INFO: LU info: Event 16 12 3 10 4 8 18 9 18 4 8
18 17 14 20 1 ,state = 5, smaState = 1
%CIP2-1-MSG: slot5 01, flag = D0
```

A workaround is to disable the configuration options that would cause the client to disconnect due to inactivity, such as keepalives and idle time. [CSCdw31269]

• The customer file transfer application reports CRC failures during the first few files transferred. Eventually, the CRC failures stop.
This bug occurs when the customer uses an increased number of receive direct memory access (DMA) buffers for the Logical Link Control (LLC) on the CIP.

The workaround is to maintain the number of DMA buffers at the default—do not configure the max-llc2-rcvbufs. [CSCdw55422]

• The CIP TN3270 server may exhibit a slow memory leak in the TN3270 server response time task.
The workaround is to stop and restart the CIP TN3270 server. [CSCdw88211]
The TN3270 server does not send an inbound NOTIFY or TERMSELF response following a NO_BIND_REQ_RCVD error.

This could occur while an LU is in the system services control point (SSCP) state (immediately following client connection or unbind/passive) and a BIND is not received within a 2.5 minute timeout. The VTAM/CICS does not clean up, so the application currently assigned to the LU remains, and the next client to connect might get an incorrect application.

There is no workaround. [CSCdx56737]

A NO_BIND_REQ_RCVD error is logged for TN3270 printers and the printers disconnect.

When a printer connects to the TN3270 server, but no print jobs are ready to be printed, the TN3270 server disconnects after 2.5 minutes and a NO_BIND_REQ_RCVD error is logged. If this occurs, subsequent printing fails because the printer is no longer connected.

The TN3270 server should not disconnect printers when a BIND is not received within 2.5 minutes. This should only occur for LU type 2 (display) clients.

The workaround is to verify whether print jobs are ready to be sent to the printer before connecting to the TN3270 server. [CSCdx58390]

Open Caveats in Version 27.20/Resolved Caveats in Version 27.21

This section describes possible unexpected behavior in Version 27.20. All the caveats listed in this section are resolved in Version 27.21.

A host receives an INOP 01 code message when a logical link control (LLC) session disconnects. This problem occurs when two VTAM systems are connected via an APPN network and an operation such as a normal disconnected mode (NDM) file transfer is processed. One end of the connection terminates the operation normally. The other end detects the LLC session disconnection and forwards a close_station_indication message with a code 7657 to VTAM. The code 7657 is translated as an abnormal disconnection sequence and causes VTAM to issue an IST1412I message with a return code 7657 and an INOP code 01.

The CIP should send a normal LLC disconnection sequence indication with a code 7656 instead. This sequence is illustrated in the following example:

```
Hosta--cip/csna-------dlsw------cip/csna----Hostb
  <-------------------appn------------------------>
```

There is no workaround. [CSCdp12204]

A CIP fatal error 35 occurs after a shutdown of the TN3270 server or the Dependent Logical Unit Requestor (DLUR) component of the TN3270 server. This problem does not occur often, but when encountered it seems related to high volume networks where the TN Server and Host are busy. In most instances, the TN Server will also log messages for the physical unit (PU) or logical unit (LU), stating it did not get a response from the Host in 30 seconds.

The fatal error occurs after issuing the shut command from routename(cfg-tn3270)# or routename(tn3270-dlur)# modes.

There is no workaround. [CSCdu03050]

A fatal error 9 can occur when running IP over Cisco Multipath Channel Plus (CMPC+) using the new ESCON Channel Port Adapter Version 4 (ECPA4) in a Cisco 7200VXR router with an Network Process Engine 400 (NPE400).

There is no workaround. [CSCdu49534]
The router syslog messages showed the following just before developing a fatal error 9.

%ECPA-3-MSG: slot4 %CMPCTG-3-LS_FSM_ERR: TG Name: P2US6092-Ls, Event ISlepiFlowStop, State SStationOpen
%XCPA-3-STATUS: bay [4] Fatal error detected (code=9)
%ECPA-3-MSG: slot4 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/ls.c @ 339 - msgP

The cause is unclear.

There is no workaround. [CSCdv25071]

The following fatal error message can occur when using the SNA-Cisco MultiPath Channel (CMPC) features:

%SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./mpc/mpc.C @ 5793 - msgP

There is no workaround. [CSCdv58115]

A Cisco router with a CIP running on the TN3270 server and CSNA reloads with the following error messages:

%SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./cta802/dlu.c @ 437 - this && this->read_q && msg
%DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)

There is no workaround. [CSCdv63166]

A 0812 and/or 0897 error message occurs in response to an Activate LU (ACTLU). This occurs more often when using the dynamic LU naming feature. The problem occurs if the VTAM/host performs an Initial Program Load (IPL) without reloading the router.

A workaround is to perform an IPL of the host, then reload the router to clean up internal data structures. [CSCdv71737]

The CIP router crashes with a fatal error 37 when the mainframe is configured for Open Shortest Path First (OSPF).

There is no workaround. [CSCdv72227]

An AS/400 TN3270 client negotiates a termtype of IBM-3487 with the CIP TN3270 server. IBM-3487 is an invalid 3270 termtype and will not handle 3270 data streams correctly.

This terminal type (along with similar models 3486, 3488, and 3489) should be rejected by the CIP.

There is no workaround. [CSCdv83239]

Open Caveats in Version 27.19/Resolved Caveats in Version 27.20

This section describes possible unexpected behavior in Version 27.19. All the caveats listed in this section are resolved in Version 27.20.

- The working window size (Ww), displayed by the `show extended channel x/2 llc oper` command might display 0 instead of the correct value.
  
  There is no workaround. [CSCdt92975]

- The binds from the Network Node Server (NNS) are rejected with sense code 08150004, LFSID in use.
Caveats for CIP and CPA Microcode

This problem only occurs with Dependent Logical Unit Requestor (DLUR) physical units (PUs). It then occurs when the link to the NNS goes down. For example, with a 3745 controller acting as the NNS, a customer can take the tic down on the 3745, or shut the CSNA channel to the host.

The TN3270 server Dependent Logical Unit Requestor (DLUR) link failure cleanup results in a condition where the local form session identifier (LFSID) is still in use, causing future (i.e. when the link recovers) BINDs from the Network Node Server (NNS) control point to be rejected with sense 08150004. This failure to clean up the LFSIDs causes internal DLUR PU processing to improperly shut down processing of the lost links. The result is that the TN3270 server does not recover the DLUR/DLUS pipe, and the TN3270 physical unit (PUs) fail to activate.

There is no workaround. [CSCdu01381]

- An ESCON CPA (ECPA) to ECPA file transfer showed a large number (30 percent), of retransmitted I-frames. Examination of the receiving CPA showed a large number of Read direct memory access (DMA) failures due to no buffers. This occurs when a large number of file transfers happen simultaneously over several concurrent logical link control (LLC) sessions.

A workaround is to use a very small window size, thereby reducing the number of retransmits, but also reducing overall throughput. [CSCdu24530]

- When a Cisco 7500 series router with a CIP card is reloaded or the microcode reload command is issued, the devices on the mainframe that correspond to the Cisco Systems Network Architecture (CSNA) or the Common Link Access to Workstation (CLAW) devices on the router might get “Boxed”. The mainframe is running OS/390, and the CS/390 version is 2.8. The following message is displayed:

```
IST1188I VTAM CSV2R8 STARTED AT 04:43:06 ON 04/08/01
```

This problem is observed in routers running Cisco IOS Release 12.1(4) or Cisco IOS Release 12.1(6), and CIP microcode Version cip27-12.

A workaround is to either have the devices varied offline on the mainframe where they are defined, or to vary the “boxed” device offline with the UNCOND option, if the reload happens unintentionally (i.e., router crash, power outage, etc.). [CSCdu26652]

- The CIP might fail with a fatal error 35 in ccb802.c.

There is no workaround. [CSCdu36395]

- Invalid MPC buffer from mainframe causes fatal error 35 on CIP.

There is no workaround. [CSCdu66303]

- Common Link Access to Workstation (CLAW) packing failed to initialize when using cip26-20 or above. There were no specific conditions for this bug.

There is no workaround. [CSCdu80489]

- Multiple console messages appear when performing a CIP reload.

There is no workaround. [CSCdv04228]

- When booting the CIP, it might take an excessive amount of time if LU nailing is being used, and a common client IP/mask combination is nailed to many physical units (PUs). The amount of time it takes varies, depending upon how many PUs/LUs the client mask is nailed to. It could take many “minutes” for hundreds of PUs, or hours if nailed to 1000 or more PUs. During this time, the CIP CPU utilization will be up around 100 percent.

There is no workaround. [CSCdv17797]
Open Caveats in Version 27.18/Resolved Caveats in Version 27.19

This section describes possible unexpected behavior in Version 27.18. All the caveats listed in this section are resolved in Version 27.19.

- When a microcode reload occurs, the router log does not indicate what version of CIP microcode is being reloaded.
  
  There is no workaround. [CSCdt82371]

- The performance for logical link control (LLC) links are greatly reduced or stopped while the link physically remains active, but little or no data flows over the session. This occurs when the customer is using two Channel Interface Processors (CIPs) between mainframe (MF) environments. They have 4 xCPAs sending Main Frames (MF) data over LLC connections in a physical unit 5 (PU5) to PU5 environment, mapping many view runners (VRs) over a single LLC2 Virtual Routes (VRs) instance. Between the two CIP routers is an OC-48 pipe. The customer desires a minimum of 40M throughput and uses large local LLC windows to accomplish it.

  Due to network congestions, packets are lost between the two CIP routers causing flow control measures to be activated. As a result, the dynamic windowing support is enabled. As part of the dynamic windowing support, the local send window is reduced, but not subsequently increased per the specification.

  The workaround is not to enable dynamic window support on CIP (llc2 nw). [CSCdu08352]

- The TN3270 Dependent Logical Unit Requester (DLUR) link fails to activate when the remote MAC (RMAC) is an Advanced Peer-to-Peer Networking (APPN) port on the same router. The BIND is rejected with sense code 80040000.

  The workaround is to change the RMAC to point to an external communications adapter (XCA), and not the APPN port. [CSCdu19516]

- If the TN3270 server receives an active physical unit (ACTPU) for a physical unit (PU) when the PU is already active, the TN3270 server does not forward the product set identification (PSID) packets inbound for logical units (LUs) which are active on the PU. The result is that the LUs do not appear as active/in-session in the virtual telecommunications access method (VTAM).

  This situation might occur in cases where the TN3270 PUs are downstream from a Dependent Logical Unit Requester (DLUR) node upstream. If the DLUR link is taken down and then re-established, the only communication to the TN3270 server is a subsequent Activate Physical Unit (ACTPU). Because no intervening deactivate physical unit (DACTPU) is sent to the TN3270 server, this results in the server receiving the ACTPU while the PU is already active.

  There is no workaround. However, this bug does not appear to present any real problems other than that the LUs do not appear as active in the VTAM status displays. Operationally, the LUs appear to function properly. [CSCdu30329]

- If the TCP port is changed for a TN3270 PU, clients can no longer connect to LUs defined on that PU.

  The workaround is to avoid reconfiguring the TCP port. [CSCdu35076]

- A router with ESCON CPA (ECPA) loses the Cisco Multipath Channel Transmission Group (CMPC TG) link and becomes inactive, for some unknown reason. The log displays the following:

  "%ECPA-3-MSG: slot4 %CMPCTG-3-LS_FSM_ERR: TG Name: WMP1B – Ls, Event IXidInd, State SConnected"

  The workaround is to perform a shut/no shut on the interface. [CSCdu40527]
• A CIP fatal error 35 appears when processing a configure-nack to an Inter Processor Communication (IPC) message.

There is no workaround. [CSCdu40818]

• The CIP router running microcode Version cip27-13 configured for Cisco Multipath Channel Plus (CMPC+) crashes with a fatal error 35.

There is no workaround. [CSCdu60678]

• Logical units (LUs), which should be free and available might not be available. Symptoms might be that “resource not found” errors are logged, or the Activate LU (ACTLU) might be rejected with an error message 0897. This problem occurs when the TN Server detects a logical unit (LU) name clash. An LU name clash might occur in the following circumstances:
  
  – Customers use the same first 6 characters for physical unit (PU) names without defining an lu-seed. The server creates default LU names by concatenating the first 6 characters of the physical unit (PU) name with the locaddr.
  
  – Customers define static LUs (at VTAM) with names that clash with the default names on the server. For example, if the server has a PU named PU1, it will name LUs (by default) so that locaddr 1 is PU1001, locaddr 2 is PU1002, etc. If the static VTAM names are inconsistent such that locaddr 2 is PU1000, locaddr 3 is PU1001, etc., this results in a name clash on the server.
  
  – Customers use dynamic lu naming, which might produce a name clash.

Note  
Name clashes are generally acceptable. The server has an algorithm which handles the clashes by renaming unclaimed LUs to avoid the clash. An error in this logic made some LUs inaccessible.

If a customer sees LU names beginning with a 4 digit decimal value (such as 0001xxxx, 0002xxxx, etc.) in the output of a show extended channel tn3270-server pu command or a tn3270 resources pu command, then the server has detected a name clash and this bug is likely.

A workaround is to avoid situations which produce name clashes such as those identified above. [CSCdv08691]

Open Caveats in Version 27.17/Resolved Caveats in Version 27.18

This section describes possible unexpected behavior in Version 27.17. All the caveats listed in this section are resolved in Version 27.18.

• A fatal error 35 is sent from the CIP TN3270 server, when TNSessionDisConnect is the last entry in the trace.

There is no workaround. [CSCdt24977]

• The TN3270 server is not cleaning up the logical unit (LU) when the following message is displayed. The LU is being reallocated for another session, and the previous login screen appears at the host.

%CIP2-3-MSG: slot4 %TN3270S-3-NO_BIND_REQ_RCVD:  
No BIND REQ received on LU xxx

There is no workaround. [CSCdt84286]

• If a particular logical partition (LPAR) on the mainframe (MF) hangs, it could cause a CIP adapter to hang and not pass traffic. This can occur when running CIP microcode Release 26-17. The CIP can hang, providing no diagnostic output to determine the condition that caused the hang.
The customer might see the following message when this occurs:

```
%IPC_RSP_CBUS-3-NOBUF: No more IPC memd buffers to transmit IPC message.
```

This problem was seen in the following environment:

CIP Release 26-17, Cisco IOS Release 12.0(9)

```
Topo:     MF-1   MF-2
        |   \
        |   /  
        |  / \ 
        |/ \
Escon Dir1 Escon Dir2
CIP rtr1   CIP rtr2
```

The CIP adapter in each CIP router hung when LPAR 4 in MF-1 hung.

The workaround is to issue a microcode reload command and/or reload the router. We had to issue the microcode reload command two times before it took effect. [CSCdt86405]

### Open Caveats in Version 27.16/Resolved Caveats in Version 27.17

This section describes possible unexpected behavior in Version 27.16. All the caveats listed in this section are resolved in Version 27.17.

- **When the USS messages are too long, the TN3270 server does not suppress the Clear key.** Instead, the TN3270 server sends it to the virtual telecommunications access method (VTAM). The VTAM answers with an error message. An inbound clear aid should be suppressed and a *write with keyboard restore* would be sent back to the client.

  The workaround is to code shorter USS messages in the USS table. [CSCdt51737]

- **The TN3270 server user logs on to a virtual telecommunications access method (VTAM) application from a USSMSG10.** This application sends the BIND and then upon receiving the BIND +RSP sends the Start Data Traffic (SDT), and gets a response. The application then waits for the user to enter a transaction ID. It does not actually send a screen (or clear screen) to the logical unit (LU). On a locally attached LU to a 3174, the 3174 clears the screen when putting the LU into the LU-LU session (previously it was in the SSCP-LU session).

  The CIP/CPA TN3270 server does not clear the screen. This leaves the screen with the USSMSG10 and USSMSG0 (“COMMAND ACCEPTED”) screen displayed at the client.

  The VTAM application needs to be one that does not initially write to the logical units (LUs) screen. No particular levels of Cisco IOS software, CIP/CPA microcode, or VTAM apply.

  The workaround is to modify the application and send out an *Erase/Write* command to the LU. [CSCdt57583]

- **After a Dependent LU Requester (DLUR) physical unit (PU) is varied inactive and active again, the logical unit (LU) allocation algorithm is altered so that the LUs are no longer allocated properly on alternating PUs.**

  The normal allocation scheme allows dynamic LUs to be allocated from a PU until a given PU has two less free LUs than the next PU. Because the server does not free up LU resources when the DLUR PU is inactivated, these previously used LUs will be allocated first upon reactivation, regardless of the load-sharing algorithm. The TN Server always uses free LUs that have resources allocated before allocating resources for any new LUs. The real problem is that the server should be freeing up LU resources for LUs that are not in session when the DLUR PU is inactivated.
The workaround is a shut/no-shut on the PU, which frees up the inactive LUs. However, this is not necessary or recommended since having the LUs allocated/inactive does not cause any problems other than affecting the method of allocating dynamic LUs. [CSCdt62248]

- A NetView Distribution Manager (NDM) data transfer was performed. When verified on the receiving end, the file contained additional records.

There is no workaround. [CSCdt70199]

Open Caveats in Version 27.15/Resolved Caveats in Version 27.16

This section describes possible unexpected behavior in Version 27.15. All the caveats listed in this section are resolved in Version 27.16.

- Bouncing transmission groups (TGs) for Cisco Multipath Channel Plus (CMPC+) frequently causes the CIP to restart with the following messages

  01:40:03:%ECPA-0-MSG:slot5 %BSQ-0-SCB_CHAIN:Read SCB chain is out of sequence
  01:40:03:%ECPA-0-MSG:slot5 %DEBUGGER-0-FATAL_ERROR:Fatal error (code=37)

  This problem is found in cip27 releases.
  The workaround is not to activate, then deactivate TGs frequently when traffic is running from the CIP to the mainframe. [CSCdk87042]

- The TN3270 server on the CIP might wait three seconds before sending a notify slu enabled message when a client requesting a nonstatic logical unit (LU) by name attempts to reconnect.

  The workaround is to code the LU termination as always. [CSCds74621]

- In defining a new physical unit (PU) at virtual telecommunications access method (VTAM), if there are static logical units (LUs) and INCLUDOe=yes, the activate logical units (ACTLUs) to those static LUs might be rejected with a 0897 sense code. This error occurs when LU names from a previously defined PU are reused when defining the new PU.

  The workaround is to remove the original PU (on which the LUs were named) from the PU definition on the router using the no PU <puname> command. [CSCdt01236]

- The Channel Interface Processor 2 (CIP2) board crashes with the following fatal error 32:

  %CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=32)

  This occurs when you enter a no pu command on a TN3270 server.

  There is no workaround. [CSCdt05019]

- If a client connects to an LU using the dynamic LU naming feature, the following type of error might occur when a user disconnects from the LU.

  %CIP2:slot3 ChangeResourceName:new name PUA01 conflicts

  Once this error occurs, the LU can only be accessed by using the name given the LU by the previous dynamic LU naming client. In some situations, a fatal error, such as that described in CSCdt01019, might occur.

  These problems occur when the server internal LU names clash, causing pseudo-names to be created. Internal names clash when the first 6 characters of a PU name on a common listen-point are the same. The server builds LU names by combining the first 6 characters of the PU name with the locaddr, so when the first 6 characters of the PU names are the same, the names clash.
A workaround is to define PU names in which the first 6 characters are unique, or use unique LU seeds on the PU definition on the server. If lu-seed is used on the server PU definitions, the recommendation is that the seed match the LUSEED defined for the PU in the Virtual Telecommunications Access Method (VTAM) PU definition. [CSCdt18308]

- When installing a new Common Link Access to Workstation (CLAW) packing feature, packstat from the CIP console does not work correctly when ELPs exceed 16.
  There is no workaround. [CSCdt42288]

- The customer configures the TN3270 server with a logical unit (LU) nailing and dynamic LU on a CIP. If a TN3270E client asks for a LU not assigned to the client, the TN3270 server should send a reject frame, as described in RFC 854. The customer has to use dynamic LU, LU nailing, and TN3270E client for this to occur.
  There is no workaround. [CSCdt44144]

- When there are too many TCP connections to a TN3270 physical unit (PU) IP address destination port 65535, the CIP crashes with the following messages:

  ┌───────────────────┐
  │ %CIP2-0-MSG: slot4│DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)27 19:00:06: │
  │ %CIP2-0-MSG: slot4 │
  │ %SCHED-0-NOPROCID: No process id available for process creation │
  │ %CIP2-0-MSG: slot4 │DEBUGGER-0-FATAL_ERROR: Fatal error (code=35) │
  └───────────────────┘

  There is no workaround. [CSCdt47389]

- After the channel has timed out on the CIP, the following output is given:

  Con should be N.

  odyssey#show extended channel 0/1 sta
  Path: 0190  -- ESTABLISHED
  Command Connects Selective System Device CU
  Dev Connects Retries Cancels Reset Reset Errors Busy
  E0 13 0 0 0 0 2 0 0
  Blocks Bytes Dropped Blk Memd
  Dev-Lnk Read Write Read Write Read Write wait Con
  E0-00 0 0 0 0 0 0 0 Y
  Last statistics 0 seconds old, next in 10 seconds

  The above occurs when the channel has timed out because the host has been stopped (i.e., “v net,cancel”).
  There is no workaround. [CSCdt47430]

- A NetView Distribution Manager (NDM) data transfer was performed. When verified on the receiving end, the file contained additional records.
  There is no workaround. [CSCdt70199]

- A fatal error 35 might occur when a no listen-point command is given while sessions are active.
  There is no workaround. [CSCdt73803]

Open Caveats in Version 27.13/Resolved Caveats in Version 27.14

This section describes possible unexpected behavior in Version 27.13. All the caveats listed in this section are resolved in Version 27.14.
- The CIP restarts with a fatal error 35 when configuring Cisco Multipath Channel (CMPC) statements with alternating no shut. This occurs if the following sequence is pasted in interface mode:

```plaintext
int ch2/1
    cmpc C040 72 TG0 READ
    no shut
    cmpc C040 73 TG0 WRITE
    no shut
    cmpc C040 74 TG1 READ
```

The workaround is to issue the `no shut` command once. [CSCdm39276]

- When trying to bring up a CLAW session while another CLAW session is active, and the Block Dropped on Read subchannel is increasing, the log displays the following message:

```plaintext
%CIP2-6-MSG: slot5 %SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
```

This condition occurs only if the following circumstances are satisfied:
- The CIP is running out of System Control Board (SCB).
- Only one CLAW device is configured or there is one device which was hit by a large number of packets in a short period of time.
- The customer is trying to bring up or tear down one more CLAW session by performing the following tasks:
  1. Shut down the interface.
  2. Perform a microcode reload.
  3. Confirm that all CLAW devices are configured.
  4. Perform a no shut.

There is a hole in the `get_scb` function, where we allocate and release SCB in the same thread. Because the CIP allocates SCB for a control message using this function, there is a potential CIP lock when the CIP is hit by the above conditions.

There is no workaround. [CSCds32524]

- When using VRN (Virtual Routing Node) to connect the TN3270 server to multiple hosts, the server attempts to create many dynamic links with a host, which fails, but uses up all its available dynamic link stations.

There is no workaround. [CSCds50942]

- Issuing the `llc stat protocol all` command on the CIP console results in a fatal error 35. Without configuring any adapters, if we issue `llc` commands on the CIP console, fatal error 35 results.

There is no workaround. [CSCdt10243]

- The TN3270 server sometimes awards a client a logical unit (LU) nailed with a shorter netmask over an LU nailed with a longer netmask. This occurs in the following two scenarios.

In the first scenario, the user configures a new client nailing statement that has a longer netmask than an existing client nailing statement that covers the same client. If the client has been awarded LUs in the past from the shorter netmask, then newer client connections will be awarded the LUs from the shorter netmask first.

In the second scenario, the configuration already contains two nailed client statements, one with a shorter netmask. If the client connects using different model types, occasionally the client is incorrectly awarded an LU from the nailing statement with the shorter netmask.
Following is a sample configuration problem fix:

```
tn3270-server
idle-time 60
keepalive 60
dlur NETA.JMK NETA.MVSD
lsap token-adapter 1
link HOSTMVSD rmac 4000.7500.7500
pu PU1 11111111 10.100.1.1
client ip 10.100.0.0 255.255.0.0 lu 224 225
pu PU2 22222222 10.100.1.1
client ip 10.100.1.0 255.255.255.0 lu 113 114
```

Prior to this fix, a client with an IP address of 10.100.1.10 would sometimes get LU 224 or LU 225 before LU 113 or LU 114. The TN3270 server should always award a nailed LU with a longer netmask over an LU with a shorter netmask.

A workaround is to perform a shut and no shut on the TN3270 server. [CSCdt18785]

---

**Open Caveats in Version 27.12/Resolved Caveats in Version 27.13**

This section describes possible unexpected behavior in Version 27.12. All the caveats listed in this section are resolved in Version 27.13.

- The counter displayed by the `show ext ch x/2 connection-map llc2` command displays the wrong number of active Logical Link Control, type 2 (LLC2) connections when the Virtual Telecommunications Access Method (VTAM) is configured to connect out through the CIP. The count matches the number of connections open when it should match the number of connections established.

  There is no workaround. [CSCdi67144]

- The CIP Logical Link Control (LLC) `WwCountChanges` counter from the `show extended channel slot/port llc statistics mac sap mac sap` command, and the `ConnectFail` counter from the `show extended channel slot/port llc statistics` are not incrementing correctly.

  There is no workaround. [CSCds29197]

- A fatal error 35 occurs when forcing the Multiple Virtual Storage (MVS) of a Primary Dependent Logical Unit Server to stop by the `QUIESCE` command. This problem is seen at any time with the `QUIESCE` command.

  There is no workaround. [CSCds72088]

- A fatal error 35 might occur if the client is in the “hold state” and attempts to reconnect to the same resource. A client enters the hold state after attempting to connect to an invalid resource or one which is not currently available 10 consecutive times. Normally, if a client again attempts to connect to the same resource, the “hold state” message occurs again. As a result of this bug, a fatal error 35 might occur instead. This problem occurs as a result of the resolution for CSCdr50532, so therefore only exists in Release 27-12.

  The workaround when the client is in the “hold state” is to attempt to reconnect to a different resource rather than attempting to reconnect to the same resource. [CSCds92038]
Open Caveats in Version 27.11/Resolved Caveats in Version 27.12

This section describes possible unexpected behavior in Version 27.11. All the caveats listed in this section are resolved in Version 27.12.

- The TN3270 server logs various messages if the TN3270 client fails to connect to the TN3270 servers on the CIP/CPA. The bug requests that the TN3270 server send messages to the TN3270 clients under various conditions.

**Note**  This is not a software bug, rather this DDTS just requests an enhancement to the TN3270 server.

The workaround is to look at the router log. [CSCdr50532]

- When the CIP receives many small packets in a very short period of time, the router freezes or locks up and receives these messages:

  %CIP2-6-MSG: slot5 %SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
  %CIP2-6-MSG: slot5 %SCB-6-RESUME: SCB on port 0 available,correlator: 0 task: CLAW read0/C700/00 8040CE10

  The workaround depends on customer network topology and configuration. [CSCdr85879]

- Previously, in legacy style configurations when a client was nailed using a client `ip a.b.c.d x.x.x.x lu` statement, the mask was applied by Cisco IOS software before being sent to the CIP. Currently, with Kirribilli-release style configurations, Cisco IOS software does not apply the mask before sending the nailing statement to the CIP. This has the following two side effects:
  1) Using masks, we can now nail the same client to different pools of logical units (LUs).
  2) Because the masks are applied by the CIP and not applied in Cisco IOS software, some client IP statements cannot be removed from configurations.

Item number one will not be addressed in this DDTS. To reproduce number two, configure the TN3270 server as follows:

```
tn3270-server
pool JEFFPC cluster layout 2s
listen-point 172.18.5.237
pu JJ1PU 90007424 token-adapter 15 14 rmac 7500.cafe.efef lu-seed JJ1PU###
allocate lu 10 pool JEFFPC clusters 1
```

Then, nail the client to pool JEFFPC with the following statement:

```
client ip 10.83.10.202 255.255.0.0 pool JEFFPC
```

Look at the nailing tables on the CIP:

```
Nailed address = 10.83.0.0, mask value 255.255.0.0
```

When you attempt to remove the nailing statement, you will receive the following message:

```
%TN3270-1-NAIL_NOT_FOUND: Deletion of the Client IP (10.83.10.202) LU\Nailing first (0) to last (0) failed because the configuration was not\found.
```

Configure an alternative to the CIP as follows:

```
no client ip 10.83.0.0 255.255.0.0 pool JEFFPC
```

The Cisco IOS software says:

```
%client ip 10.83.0.0 is not configured.
```
To remove the client IP statement you must reload IOS. 
There is no workaround. [CSCds23641]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with a fatal error 9 because a corrupted or runt MPOA Client (MPC) frame has been received.

```
%CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/mpc.C
@ 2049 - ssi_msg_length( bfrP) >= (sizeof( MpcFra
%CIP2-3-MSG: slot0 memHdr) + frameSize)
%CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

There is no workaround. [CSCds27703]

- Once a logical unit (LU) is disconnected, the client cannot reconnect for 10 seconds. This happens when the tn-server, listen-point, or physical unit (PU) is configured for lu deletion never, which is the default value. After an LU disconnects, the server waits for 10 seconds for the host to respond to an inbound power-off product-set identification (PSID). However, when lu-deletion is set to “never”, no PSID request is sent inbound, so no host response will be received. The fix is to configure lu deletion always. This forces the power off PSID to be sent inbound. 
There is no workaround. [CSCds28146]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with the fatal error 9 below when a virtual CIP adapter is removed that is part of an active transmission group (TG).

```
%ECPA-3-MSG: slot3 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/clean.C
@ 372 - elemP
%ECPA-0-MSG: slot3 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

The workaround is not to remove adapters for TGs without first inactivating the TG from the host system. When defining TGs, make sure all adapters are configured first. [CSCds32606]

- The NO_LU_SESSIONS message which appears when a client requests connection to a generic logical unit (LU) when no generic LUs are available does not contain data to indicate which client is attempting the connection. Also, after 10 such attempts, the client should be put into a hold state rather than being allowed to continually attempt the connection to an unavailable resource. The client attempts to connect to a generic LU, but no generic LUs are available.

These are cosmetic changes to the error message that is displayed when no LUs are available, so there is no bug to workaround. The following message is currently displayed on the router console when a client attempts connection to a generic LU and none is available:

```
%CIP2-4-MSG: slot4 %TN3270S-4-NO_LU_SESSIONS: No LU sessions left in :GENERIC for PUs at IP addr 172.18.5.202, port 23
```

This message will be enhanced to give an indication of the client that attempted to connect. The modified message shall be as follows:

```
%CIP2-4-MSG: slot4 %TN3270S-4-NO_LU_SESSIONS: Client session 10.83.120.43:1195 requested a generic LU from IP 172.18.5.202:23, but no LU is available.
```

Additionally, if 10 such connect attempts are made from the same client, the client will be put into a hold state and the following message will appear on the client screen:
THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.

There is no workaround. [CSCds33140]

- The fatal error 35 occurred in cip27-5 and above when the command `no pu puName` was executed. This occurs only when one of the logical units (LUs) is in a hold state and this command is executed. This fix helps prevent the crash from happening.

There is no workaround. [CSCds39875]

- The CIP card configured for Cisco Multipath Channel (CMPC) hangs with the following messages:

  \[
  \text{%RSP-3-RESTART: interface Channel0/2, output stuck} \\
  \text{%LINEPROTO-5-UPDOWN: Line protocol on Interface Channel0/2, changed state to down}
  \]

  The problem can also be seen by performing a “tasks” command on the CIP console when the central processing unit (CPU) is at 100 percent. Both symptoms are triggered by adding new Cisco Multipath Channel Transmission Groups (CMPC TGs) or the flapping of existing TG(s).

  A potential workaround is to add new TG(s) only during a maintenance window and update the configuration immediately following a reload of the microcode. [CSCds41393]

- When a client disconnects, and the server is configured for `lu termination termself`, the server always sends the inbound TERMSELF, byte 3, as 0x44 indicating forced termination. To avoid operator intervention upon subsequent connect, this should be sent inbound as 0x4C, indicating cleanup. Similarly, when configured for `lu termination unbind`, the UNBIND always flows inbound with byte 1 = 0xFE, indicating session failure. This should be 0x0F, indicating cleanup.

  There is no workaround. [CSCds44696]

- The CIP/CPA restarts with a fatal error 35 when a transmission group (TG) is configured with an adapter number that exceeds the limit of 18. This occurs at all CIP/CPA code levels.

  The workaround is not to exceed the limit of total number of adapters that can be associated with all TGs, that is, 18. [CSCds47000]

- A fatal error 32 can occur when deleting a transmission group (TG) for Cisco Multipath Channel Plus (CMPC+) and then reconfiguring it.

  There is no workaround. [CSCds48048]

- The TN3270 server translates systems network architecture (SNA) type commands to their non-SNA version before being sent to the TN3270 client. For example:

  \[
  \begin{align*}
  0xF5 \text{ is translated to } 0x05 \\
  0xF1 \text{ is translated to } 0x01 \\
  \end{align*}
  \]

  and so on.

  This DDTS request is for a command to allow users not to have this translation occur. When configured properly, the SNA version of the TN3270 commands would flow through to the client unmodified.

  There is no workaround. The TN3270 server always translates the commands. [CSCds48150]

- The TN3270 server is configured with both static and dynamically created logical units (LUs). Physical units (PUs) are created under listen points. The following fatal error 35 occurs in the TN3270 Response Time Work Thread:

  \[
  \text{%CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)}
  \]

  There is no workaround. [CSCds49209]
The TN3270 client configured for VT100 ANSI terminal should not be able to negotiate a session with TN3270 server. This terminal type will be added to the list of unsupported terminal types.

There is no workaround. [CSCds51099]

The TN3270 clients that are nailed to dynamic Logical Units (LUs) might be unable to reconnect once the LUs are placed on the TN3270 server bad queue. This could happen if the LU has been inactivated (Deactivate Logical Unit, or DACTLU) when the client previously connected. The server mistakenly might think the LU has been varied inactive (via Virtual Telecommunications Access Method, or VTAM), and will not allow subsequent reconnection to the LU.

The workaround is once the LU is in this state (on the bad queue and the server will not allow reconnection), the only recovery is shut/no-shut on the PU, or to vary the PU as inactive/active. To avoid this situation, one might code `lu deletion never`, so that DACTLU does not flow when a client disconnects from the LU. [CSCds67701]

Open Caveats in Version 27.10/Resolved Caveats in Version 27.11

This section describes possible unexpected behavior in Version 27.10. All the caveats listed in this section are resolved in Version 27.11.

Clients attempting to connect to a CIP TN3270 server using pooled Logical Units (LUs) might receive the following message:

**THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.**

The LUs are statically defined to virtual telecommunications access method (VTAM) and `lu-deletion never` and `lu termination termself` are coded. The LUs during the session termination process are not always returned to the pool. Eventually the pool runs out of LUs and the above message is displayed at the client.

The workaround is to enter the following commands from the CIP/CPA console:

```
if-con cip_slot c
  tn3270 option nmvtpsid 0
if-quit
```

These commands will not live through a router reload or microcode reload. [CSCdr66536]

A fatal error 35 crash occurs on the CIP, TN3270 server, or virtual interface, shutting it down. There is no workaround. [CSCdr73141]

A fatal error 32 occurs when issuing the `tasks query` command from the CIP console with the wrong process ID number.

There is no workaround. [CSCdr74632]

The TN3270 server assigns available logical units (LUs) in a Round-Robin fashion—that is, LU #1 is given to the first connecting client, LU #2 is given to the next connecting client, etc. This algorithm is followed regardless of the state of lower-numbered LUs. This Round-Robin assignment requires customers to configure all 255 LUs per Physical Unit (PU) to end-applications such as CICS.

The workaround is to configure the necessary LUs to the applications. There is no other workaround. [CSCdr89694]
Caveats for CIP and CPA Microcode

- The Cisco Multipath Channel Transmission Groups (CMPC TGs) get stuck in the **SAttachSapPending State**. This occurs if multiple CMPC TGs share the same service access point (SAP) on an adapter. At times only one transmission group (TG) will get the `attachsap.cfm` message. The other TGs will remain in the **SAttachSapPending State** and will not become active. The workaround is to inactivate and then reactivate the LS major nodes for affected TGs. [CSCdr87920]

- The CIP code crashes with a fatal error 35, and the microcode reloads automatically. There is no workaround. [CSCdr90593]

- The printer does not respond to data flow when the TN3270 server holds the keyboard restore until a **change direction** command is received. Two new options have been added to allow new keyboard restore functionality.

  The following options are now available:

  - **tn-parameter code 7**—Enables functionality per CSCdm93990; the server does not manipulate keyboard restore on chained WSFs, for all type devices.
  - **tn-parameter code 11**—Server does not manipulate keyboard restore on WSF, Write, and E/W commands for printers only.
  - **tn-parameter code 12**—Server does not manipulate keyboard restore on WSF, Write, and E/W commands for displays only.

  All three of the commands can be enabled to provide totally nonmanipulative keyboard restore data stream flow. Client: Attachments 6.4 and 6.5.

  There is no workaround. [CSCdr93053]

- When running the offload feature on a Cisco 7500 series router with a CIP and IBM TPF mainframe, the following message might be encountered:

  ```
  %CIP2-4-MSG: slot0 %OFFL-4-BADDESC: Socket descriptor 3 in request is bad: state DESC_Holddown compare 3
  ```

  This message is a warning to show that CIP receives an offload request command for a socket which already closed or does not exist anymore. The message does not cause any negative impact to the network or the mainframe.

  There is no workaround. This DDTS is related to CSCdp84965. [CSCdr98652]

- The customer is using the CIP TN3270 server with dynamic logical units (LUs) pooled into several pools as well as unpool GENERIC. **Generic-pool deny** is not specified for this physical unit (PU). After a Virtual Telecommunications Access Method (VTAM) restart, users cannot connect to PUs that have their LUs in the GENERIC pool. The following message is seen in the router log:

  ```
  %CIP2-4-MSG: slot1 %TN3270S-4-NO_LU_SESSIONS: No LU sessions left in :GENERIC for PUs at IP addr x.x.x.x, port 23
  ```

  A shut/no shut of the PU is required to allow users to obtain a session with one of the LUs under this PU.

  There is no workaround. [CSCds00536]

- The CIP TN3270 server might produce the following message:

  ```
  %TN3270S-6-BADTIMER: Bad timer operation(1),ra=8006AF14,funcPtr=0,oldFuncPtr=80B6E5AC
  ```
Note

The values for `ra` and `oldFuncPtr` might be different. This message can appear if the server is configured for `lu deletion termself`. Unless other problems are noted, the message might be ignored. This DDTS applies only to BADTIMER messages with operation(1).

There is no workaround. [CSCds00674]

- When using a CIP on a Cisco 7500 series router or a CPA card on a Cisco 7200 series router, the Cisco Mainframe Channel Connection (CMCC) might crash with a fatal error. This is seen only in rare situations when the free memory in the CMCC is either completely utilized or highly fragmented.

  The workaround is to increase the memory on the CMCC. [CSCds05651]

- A fatal error 35 occurs when removing the TN3270 server DLUR configuration on the shutdown virtual channel interface.

  There is no workaround. [CSCds14146]

- Cisco 7000 series routers running TN3270 servers might rarely encounter a fatal error 35 as a result of an unexpected system reload.

  There is no workaround. [CSCds16631]

- The Channel Interface Processor Common Link Access to Workstation (CLAW) packing hangs when the CIP CLAW packing receives an Internet Protocol (IP) packet which is larger than the negotiated CLAW frame size minus the CLAW packed header size.

  The workaround is to configure the IP Maximum Transmission Unit (MTU) where the size would be negotiated packet frame size (cross check with PROFILE TCPIP definition in the mainframe) minus 4 (the packed header size). [CSCds24793]

- When using Cisco 7000 series routers, issuing `show` commands for Logical Link Control (LLC) causes other `show` commands to report incorrect data rather than the current configured data. Customers should configure the LLC and issue the `sh ext ch x/y conn llc ext ch llc stats` command. This causes all other `show` commands to report Cisco IOS default data instead of the currently configured data. This problem only occurs on CIP/xCPA ucode Interim builds after 216-116 and up to, but not including, 216-130.

  The workaround is not to issue the `CIP/xCPA LLC display` commands on the affected releases. [CSCds26217]

- Clients who request a generic logical unit (LU) can be incorrectly awarded a static LU even when they are not nailed to this static LU. This occurs when the previous connection was a static LU, and there is a mix of static and dynamic LUs on a listen-point.

  The workaround is for a client to specify a dynamic LU from this physical unit (PU) and then disconnect from the dynamic LU. Then the next request for a generic client will be awarded the lowest `locaddr` dynamic LU available. [CSCds26854]

- Once a logical unit (LU) is disconnected, the client cannot reconnect for 10 seconds. This happens when the tn-server, listen-point, or physical unit (PU) is configured for `lu deletion never`, which is the default value. After an LU disconnects, the server waits for 10 seconds for the host to respond to an inbound power-off product-set identification (PSID). However, when `lu-deletion` is set to “never”, no PSID request is sent inbound, so no host response will be received. The server leaves the LU in this wait state for 10 seconds before a subsequent client can connect.

  The workaround is to configure the `lu deletion always` command, which forces the power off PSID to be sent inbound. [CSCds28146]
- A fatal error 35 appears from the CIP TN3270 server, when the server tries to send a -RSP to a Start Data Traffic (SDT), but the client disconnects while waiting for a timing mark before sending the response.

The workaround is not to configure the timing mark under the TN3270 server scope. [CSCds31131]

### Open Caveats in Version 27.9/Resolved Caveats in Version 27.10

This section describes possible unexpected behavior in Version 27.9. All the caveats listed in this section are resolved in Version 27.10.

- The TN3270 server disconnects the session. This occurs when a client connects to a dynamic logical unit (LU) that has received a Deactivate Logical Unit (DACTLU) message. The TN3270 server requests an Activate Logical Unit (ACTLU) response and starts a two-minute timer. A timer value of this length is invalid because the LU has been deactivated by the Virtual Telecommunications Access Method (VTAM) console operators. The TN3270 server does not receive the ACTLU response within the timer period and disconnects the session.

The workaround is to configure the TN3270 server to assign a different LU. [CSCdk30136]

- A fatal error 9 occurs in CIP microcode Release 26-8. The specific function that contributes to this is unknown.

There is no workaround. [CSCdr07060]

- A fatal error 35 was received when attempting to run large numbers of sessions in a test lab environment. The specific failure occurs when there is no available memory to service a new session request. The fix checks an existing kernel routine to determine the available memory. If insufficient memory exists, client connections will be rejected, and unsolicited Activate LU (ACTLU) requests from the host will also be rejected.

There is no workaround for this bug. [CSCdr07326]

- After performing an Initial Program Load (IPL), a Cisco Multipath Channel (CMPC) connection does not reactivate unless the virtual telecommunications access method (VTAM) Major Node is recycled. A `Z net,quick` command was issued in VTAM.

The mainframe at the Cisco 7200 router site is IPLed (`VTAM Z net,quick`) and the CMPC connections show PCTD2 on this host. On the Cisco 7513 host they are PREQC.

The workaround is to cycle the VTAM major node at the PCTD2 side. [CSCdr07387]

- A BADTIMER message appears when starting the TN3270 server. The messages do not impact normal TN3270 server operations.

There is no workaround. [CSCdr11353]

- The available logical unit (LU) count displayed in the `show extended channel tn3270` command output is incorrect. This problem occurs when the same static LU receives an active physical unit (ACTPU) message within 3 seconds of receiving a deactivate physical unit (DACTPU) message. This problem occurs after configuring a `z net, cancel` Virtual Telecommunications Access Method (VTAM) command, or after the initial program loading (IPL) of the logical partition (LPAR).

There is no workaround. [CSCdr40633]

- A request/response unit (RU) length error, systems network architecture (SNA) sense data 10020000, is issued by Virtual Telecommunications Access Method (VTAM). VTAM is receiving a positive bind response whereby data is missing from the end of the SNA RU. Interrogation of the
data in the bind response shows that it is missing the SLU name. As a result, the host LU is marked unusable. Not every bind response is in error, but the pattern continues over a period of time, until all host LUs are marked unusable.

While not every bind response is in error, this pattern will continue over a period of time, until such time that all host LUs are marked unusable. Additional investigation of the frame shows corruption of the data at the end of the packet. Subsequent efforts to capture documentation of the problem have revealed the same bytes for corrupted data, hex 3A through hex 3F followed by random data. Data corruption is the result of processing a spanning explorer frame from os2ping.exe (OS/2 workstation utility) with a 64 byte payload, hex 00 through hex 3F.

The workaround is not to run the OS2PING.EXE to the CIP Media Access Control (MAC) address. [CSCdr42284]

- The TN3270 server times out and the client hangs. The following example illustrates this problem:

  tn3270-server
  pu pu1 91903315 172.18.4.18 tok 16 08
  client ip 10.2.20.20 lu 10
  pu pu2 91913315 172.18.4.18 tok 16 0C

  This problem occurs when:

  - A client with the internet protocol (IP) address 10.2.20.20 activates two physical units (PUs) and gets logical unit (LU) 10. PU1 is not active. PU2 is active and the listen-point with the address 172.18.4.18 is active.
  - The autoreconnect function activates and the client attempts to connect.
  - The connection is rejected because physical unit 1 (PU1) is not active. PU1 is activated. The client autoreconnect should succeed but does not.
  - The product-set identification (PSID) reply message on network management vector table (NMVT) does not go inbound, but the server still waits for the PSID response. The TN3270 server then times out and the client hangs.

  The workaround is to disable the autoreconnect feature on the TN3270 client. [CSCdr50907]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with multiple fatal error 35 messages. This problem occurs when running Cisco IOS Release 12.0(10) and CIP or CPA microcode Version 26-10 or later.

  There is no workaround to this problem. [CSCdr54396]

- Kirribilli-style pooled logical units (LUs) are not reflected in the “available-lu” count if the generic-pool = deny. LUs must be allocated to a Kirribilli pool and the generic-pool must = deny.

  There is no workaround. [CSCdr63973]

- The customer received a fatal error 35 from the CIP during normal running conditions. No commands were being entered at the time. A bug in the TN Server software allows for non-Request For Comments (RFC) compliant negotiation exchanges to occur. Some of these exchanges have the potential to cause a fatal error 35 in the TN Server code, due to a NULL pointer reference.

  There is no workaround. [CSCdr64719]

- A systems network architecture (SNA) physical unit five (PU5) to PU5 connection going through the CIP routers does not always recover after an outage is experienced in the downstream network. This problem is usually seen when there is no autogen lines coded in the external communications adapter (XCA), which is typically done for PU5 to PU5 connections because the lines and PUs are hard coded.
This problem has also been seen with PU2.0 and PU2.1 connections. The symptom is you will not see the CIP respond to the incoming test poll.

A workaround is to recycle the XCAs after doubling or tripling the number of autogen lines. [CSCdr65638]

- An AS/400 TN3270 client negotiates a termtype of IBM-3486-BA with the CIP TN3270 server. IBM-3486-BA is an invalid 3270 termtype and will not handle 3270 data streams correctly. This fix adds IBM-3486-BA to the list of known invalid termtypes in the CIP TN3270 server. The CIP will send a WONT TERMTYPE message and allow the client to negotiate a valid termtype.

There is no workaround. [CSCdr65906]

- Clients attempting to connect to a CIP TN3270 server using pooled logical units (LUs) might receive the following message.

  THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.

The LUs are statically defined to VTAM and lu-deletion never and lu termination termself are coded. The LUs during the session termination process are not always returned to the pool. Eventually the pool runs out of LUs and the above message is displayed at the client.

The workaround is to enter the following commands from the CIP/CPA console:

  if-con cip_slot c
  tn3270 option nmvt_psid 0
  if-quit

  These commands will not live through a router reload or microcode reload. [CSCdr66536]

- The Kirribilli-style pooled logical unit (LU) is not available after Deactivate Logical Unit (DACTLU)/Activate Logical Unit (ACTLU). The LU must be allocated to a Kirribilli pool.

There is no workaround. [CSCdr70394]

- The Cisco Multipath Channel (CMPC) at times was not processing the attach sap confirm message properly when a local systems network architecture (SNA) major node for a CMPC Transmission Group (TG) was activated. The symptom for this problem is:

  %CMPCTG-3-LS_FSM_ERR: TG Name: MVSG2 -Ls, Event IXidInd, State SOpeningStation (A CMPC TG gets stuck in the SOpeningStation)

  The workaround is to deactivate and reactivate the local SNA major node. [CSCdr75344]

- The available logical unit (LU) counter can be incorrect if the systems with multiplicity (SWM) node with dynamic logical units (LUs) is rendered inactive while clients are in session and these clients have auto-reconnect configured. We believe this could be caused by the dynamic Activate Logical Unit (ACTLU) timer not expiring as it should, which results in LUs not being made available.

  The workaround is to configure clients so as not to use auto-reconnect. If this happens, a shut/no shut on the TN3270 server will restore the LUs. [CSCdr83354]
Open Caveats in Version 27.8/Resolved Caveats in Version 27.9

This section describes possible unexpected behavior in Version 27.8. All the caveats listed in this section are resolved in Version 27.9.

- The TN3270 server disconnects the session. This occurs when a client connects to a dynamic logical unit (LU) that has received a DACTLU message. The TN3270 server requests an ACTLU response and starts a two-minute timer. A timer value of this length is invalid because the LU has been deactivated by the VTAM console operators. The TN3270 server does not receive the ACTLU response within the timer period and disconnects the session.

  The workaround is to configure the TN3270 server to assign a different LU. [CSCdk30136]

- Users are unable to start new Cisco Mainframe Channel Connection (CMCC) sessions. The results of a `show extended channel x/2 tn` command indicate that some PUs are in an ACT/Busy state. The results of a VTAM display of the PU show that the PU is in an active state.

  The workaround is to reload the microcode. [CSCdm44279]

- When a parallel link that connects a Cisco TN3270 server to another server that carries the control point-to-control point sessions goes down, the Cisco TN3270 cannot establish a control point-to-control point session with any server.

  The workaround is to define alternate links to the same VTAM host only at the host end, or avoid multiple links to the same VTAM host. [CSCdp02702]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with a fatal error 9.

  CIP2-3-MSG: slot0 %SS1802-3-FATAL_ERROR: SS1_ASSERT failure in ../ssi/ssi_buff.c @ 1035 - msgP->m_next
  Jan 31 15:40:12: %CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)

  There is no workaround. [CSCdp84989]

- VTAM issues a V NET.INACT,TYPE=GIVEBACK message. The control point-to-control point session moves to the other DLUS, but the DLUR pipe stops and restarts on the same host.

  There is no workaround. [CSCdr28173]

- The last logical PU in an IP pool of listen points is placed into the WAIT state. This problem occurs when changing the TCP port while PUs are in an ACTIVE state.

  The workaround is to shutdown and restart the TN3270 server using the `shutdown` command. [CSCdr30174]

- TN3270 server logical unit (LU)s cannot be used. This problem occurs when the TN3270 server does not clear the indication that LUs were nailed during processing and delete the nailing definition.

  The workaround is to avoid manipulating nailing definitions without issuing the `microcode reload` command. [CSCdr32205]

- The Offload socket response on the transaction processing facility (TPF) is delayed by 10 seconds or more. This problem occurs when there is a lack of MEMD buffers on the channel interface on the Cisco 7500 series router for a prolonged length of time. This applies to the CIP only.

  There is no workaround. [CSCdr33661]

- The TN3270 server inconsistently names the TN3270E clients. Sometimes the name is a fully-qualified APPN name such as NETA.BTEST001. At other times the name is the local logical unit (LU) name, such as BTTEST001.

  There is no workaround. [CSCdr38323]
- The TN3270 server uses an incorrect default value of 30 minutes for the keepalive timer’s maximum response time. This problem occurs when the `keepalive` command is configured without specifying any values for the `nop` or `timing-mark` or `max-response-time` parameters.

  The workaround is to configure the `nop` or `timing-mark` parameters. [CSCdr59806]

- This is an enhancement to the Cisco MultiPath Channel Plus (CMPC+) code. The enhancement permits data packing, which could improve performance depending on traffic characteristics.

  There is no workaround. [CSCdr03076]

- The CIP fails with a fatal error 35. This occurs when the `shut` command is configured on an TN Server with active sessions.

  There is no workaround. [CSCdr33930]

Open Caveats in Version 27.7/Resolved Caveats in Version 27.8

This section describes possible unexpected behavior in Version 27.7. All the caveats listed in this section are resolved in Version 27.8.

- The TN3270 server loses pool-based logical unit (LU) nailing information. This problem occurs when the `no shutdown` command is configured multiple times on the same PU.

  The workaround for customers who are using pool-based LU nailing is to avoid configuring the `no shut` command multiple times on the same PU. [CSCdm24372]

- A user receives another user session when both users are logged into the same applications owning region (AOR) in the Customer Information Control System and that AOR is manually cancelled.

  The workaround is to not disconnect a client during the logon process; that is, after requesting an application from the SSCP screen, but before establishing the LU-LU session with that application. [CSCdm51110]

- The following message appears on the Cisco Mainframe Channel Connection (CMCC) console:

  `bad error-code 12 given`

  This valid error code indicates a missing TERMSELF response. The code to log and format this specific error into a console message is missing.

  There is no workaround. [CSCdm55961]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with error message 32. This problem occurs when the TN3270 server is configured and is using, or has used, the TN3270 monitor or a similar product.

  The workaround is to not configure the TN3270 monitor or a similar product. [CSCdp16086]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 35. This problem occurs when the `no client ip ipaddr [ipmask] pool poolname` command is configured when using logical unit (LU) pooling. The command configuration causes memory corruption and the CMCC failure. The failure usually occurs because the TN3270 server attempts to access ODD addresses when EVEN addresses are expected.

  There is no workaround. [CSCdp18803]

- The TN3270 server disconnects a TCP session after sending an “in use” message. This problem occurs when OpenConnect clients are configured to negotiate multiple logical unit (LU) names by using a device list used by the client.

  The workaround is to configure the OpenConnect client to use a single device name. [CSCdp24684]
- The TN3270 server `show pu` command output is missing logical unit (LU) states. The missing states are displayed as P-RESET. This bug also applies to the LU state objects in the TN3270 server MIB. There is no workaround. [CSCdp51038]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 32. This problem occurs when approximately 25 or more DLUR links are configured. The reply buffer is too small to contain all of the Cross Domain Initi vectors and the positive locate reply.

  The workaround is to configure fewer DLUR links. [CSCdp79125]

- The Cisco Mainframe Channel Connection (CMCC) adapter might fail when the `shutdown` command is configured in TN3270 submode.

  There is no workaround. [CSCdp99538]

- The Cisco Mainframe Channel Connection (CMCC) adapter configured for Cisco Systems Network Architecture (CSNA) might not respond to a test poll. This problem occurs because there is a miscount of the available IBM VTAM external communications adapter (XCA) resources. Typically an XCA autogen parameter is configured to automatically generate lines and PUs. This is not required for PU5-to-PU4 or PU5-to-PU5 communications.

  The workaround is to recycle the XCA major node. [CSCdr03103]

- The TN3270 server running on TPF returns the following error message:

  ```
  Offload time out
  ```

  This problem occurs when the client establishes a connection to the server, issues a request, gets the response and then closes the connection by sending a RST (reset) segment.

  The server issues a read to the connection; the read message is blocked and returns with the error message. The read message should return with a 0 message, meaning that the connection was closed. This problem happens after one minute.

  There is no workaround. [CSCdr05011]

- The logical unit (LU) number in the `show extended channel tn3270-server` command output decreases every time a client fails to telnet. Once the LU number reaches zero, clients cannot telnet to the TN3270 server although LUs are available.

  There is no workaround. [CSCdr09662]

- Unless the Definite Response option is set in the request/response unit (RU) from the host, nothing which can measure IP response time is sent to the client. This problem applies to response times obtained from the TN3270E-RT-MIB, or by using the TN3270 server show commands.

  The workaround is to use only Definite Response flows. [CSCdr10939]

- The TN3270 server allows a client to access logical units (LUs) which are nailed to another subnet.

  There is no workaround. [CSCdr12567]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with the following error message:

  ```
  %ECPA-4-MSG: slotx %TN3270S-4-NO_LU_SESSIONS
  No LU sessions left in :GENERIC for PUs at IP addr xxx.xxx.xxx.xxx, port 23
  ```

  The TN3270 server PU output displays skipped logical units (LUs). The TN3270 server does not select these LUs. All other LUs are set to ACT/SESS. Note that there is no LU display for lu4 and lu9.

  ```
  lu name client-ip:tcp nail state model frames in out idle for
  1 ABCD2001 xxx.xxx.xxx.xxx:1042 N ACT/SESS 3278S5E 38418 19615 0:6:6
  2 ABCD2002 xxx.xxx.xxx.xxx:1043 N ACT/SESS 3278S2E 21473 14085 0:18:11
  3 ABCD2003 xxx.xxx.xxx.xxx:1665 N ACT/SESS 3278S5E 9992 6147 0:0:6
  ```
The workaround is to add more PUs to the TN3270 server and VTAM configuration. [CSCdr13016]

- The TN3270E client cannot connect when it specifies PAC04 as the logical unit (LU). This problem occurs when a direct PU is named PAC and an LU seed is named PAC##. Incorrect LU names such as PAC001, PAC002,... PAC255 (note decimal local addresses) are generated. The PAC04 name is not found and the connection is refused.

  The workaround is for the TN3270E client to specify PAC004 instead of PAC04. [CSCdr13524]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with the following fatal error 35:

  `%CTA-0-INACTIVE: PA1 CTA 7C00-50 reset after being inactive for 180 seconds`

  The workaround is to shut down the CSNA subchannel before shutting down VTAM. [CSCdr13804]

- The logical unit (LU)-available number in the `show extended channel tn3270` command output is incremented on inactive PUs when adding nailing configuration commands.

  The workaround is to ignore or activate the PU to correct the lu-available number. [CSCdr17334]

- The TN3270 server improperly releases nodes which had not been deleted from the resource AVL tree. This problem occurs when the TN3270 server is restarted by configuring the `shutdown` and `no shutdown` TN3270 commands.

  A workaround is to avoid restarting the TN3270 server when there is a heavy processing load. [CSCdr18250]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 35. This problem occurs when the `no listen-point` TN3270 server command is configured.

  There is no workaround. [CSCdr19257]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 7. This problem occurs when the client disconnects after the response time group is removed from the configuration. This occurs when the response time group and the subnet are configured.

  The workaround is to remove the response time group configuration. [CSCdr20842]

- When using the TN3270 server monitor or a similar product such as SOLVE:Netmaster for TCP/IP, the length of the message fragment field is reported incorrectly. The field length is reported as “18”. It should be reported as “20”. The message fragment field is defined as follows:

```
struct {short PACKED(pktLength); short PACKED(len);
 unsigned char PACKED(bytes[16]);}
```

  This is a cosmetic failure and is present in all CIP and CPA microcode releases.

  There is no workaround. [CSCdr24412]

- VTAM issues a V NET,INACT,TYPE=GIVEBACK message. The control point-to-control point session moves to the other DLUS, but the DLUR pipe stops and restarts on the same host.

  There is no workaround. [CSCdr28173]

Open Caveats in Version 27.6/Resolved Caveats in Version 27.7

This section describes possible unexpected behavior in Version 27.6. All the caveats listed in this section are resolved in Version 27.7.
• In the output of the `show ext cn/2 pu/lu` command, some “dddlu” logical unit (LU) names appear blank if host applications send NULL slu data in the bind.  
  There is no workaround. [CSCdj90734]

• Users are unable to start new Cisco Mainframe Channel Connection (CMCC) sessions. The results of a `show extended channel x/2 tn` command indicate that some PUs are in an ACT/Busy state. The results of a VTAM display of the PU show that the PU is in an active state.  
  The workaround is to reload the microcode. [CSCdm44279]

• A Cisco Multipath Channel (CMPC) TransmissionGroup (TG) does not activate and the following duplicate group token message is returned:  
  Get CMPCP_DUPL_TOKEN:  
  This problem occurs when bringing up a TG from the host that is activating a transport resource list entry (TRLE) and when multiple TGS are configured with paths to multiple mainframes via a director.  
  The workaround is to activate the TRLE again. [CSCdp66330]

• The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 32. This problem occurs when approximately 25 or more DLUR links are configured. The reply buffer is too small to contain all of the Cross Domain Init vectors and the positive locate reply.  
  The workaround is to configure fewer DLUR links. [CSCdp79125]

• The Cisco Mainframe Channel Connection (CMCC) adapter running CIP Offload returns the following error message:  
  %CIP2-4-MSG: slot0 %OFFL-4-BADDESC: 0/9300/60 Socket descriptor 259 in request is bad: state DESC_Holddown compare 259  
  This is a cosmetic problem that should not impact performance.  
  There is no workaround. [CSCdp84965]

• The Cisco Mainframe Channel Connection (CMCC) adapter running CIP Offload reloads with a fatal error 35. This problem occurs when too many Offload and CLAW statements are configured on the same interface. The process table is shared by two interfaces and cannot exceed 530 processes. Each Offload uses 4 processes. Each CLAW uses 2 processes. There are about 20 to 30 processes that are always running in addition to any Offload or CLAW configurations.  
  The workaround is to configure fewer Offload and CLAW statements. [CSCdp85560]

• The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 32. This problem occurs when changing the IP address of a loopback interface.  
  There is no workaround. [CSCdp85890]

• There is a 10-second delay from the time that the host application sends a SHUTDOWN message until the TN3270 server responds with the SHUTC RU message. This delay applies to printer emulators and should not apply to screen devices.  
  There is no workaround. [CSCdp90214]

• A Cisco Mainframe Channel Connection (CMCC) adapter error occurs when host-defined logical unit (LU) names for one PU conflict with implicit LU seed-derived names on another PU.  
  The workaround is to avoid name conflicts by specifying `lu-seed` names on every PU in the configuration that does not overlap with the host-defined names. [CSCdr06007]

• The TN3270 server logical unit (LU) goes into P-RESET mode. This problem occurs when the server closes a client connection that is using a static LU due to an inactivity or keepalive timeout. The server sends an unbind message to the host and then waits 6 seconds before sending a
Notify/Unavailable message. If the same client attempts to reconnect within that time window and the System Service Control Point (SSCP) logon screen is received after the reconnect, but still within that window, the TN3270 server locks up. This problem occurs because the accepted SSCP screen stops the timer that would normally send the Notify/Unavailable message. Also, the SSCP logon screen will be rejected with an 0x0831 sense code.

The workaround is to reject any connect requests for that LU until the Notify/Unavailable message transmission is complete. [CSCdp66402]

- The logical unit (LU) termination setting is incorrect in SNA-NAU-MIB. The snaLuAdminTerm and snaLuOperTerm objects are set to unbind even if termself is configured.
There is no workaround. [CSCdp88662]

Open Caveats in Version 27.5/Resolved Caveats in Version 27.6

This section describes possible unexpected behavior in Version 27.5. All the caveats listed in this section are resolved in Version 27.6.

- BADTIMER messages appear when running the TN3270 server. In this case, the messages appear because a TN3270 session is being negotiated or recently has been negotiated. The messages do not impact normal TN3270 server operations.
There is no workaround. [CSCdk2163]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with error message 37. The following error messages appear:

```
%CONFIG-3-WORKLEFT: Work pending on work queue when device terminated
%DEBUGGER-0-FATAL_ERROR: Fatal error (code=37)
```

There is no workaround. [CSCp54593]

- The tn-parameter code codevalue command incorporates a code value of three. PUs configured on the TN3270 server request activation by sending ReqACTPU (DLUR PUs) or TEST/XID (Direct PUs) messages to the host. When the TN3270 server and its PUs are in backup or standby mode, the PUs should not request activation. The PUs must wait to be activated by the host.
To enable this passive activation, enter the tn-parameter code codevalue command with a code value of 3. This command tells the Server to put all PUs in a waiting state and not to send ReqACTPU or TEST/XID messages to the host. [CSCdm80770]

- In duplicate MAC environments, idle Systems Application Architecture (SAA) gateway sessions terminate. SAA gateways time out the route to the Cisco Mainframe Channel Connection (CMCC) MAC address and send receive ready poll (RR(P)) single route explorer (SRE) messages to rediscover the route. The CMCC adapter is not in session and responds to the RR(P) messages with a disconnect mode final (DM(F)) message. The SAA gateway then disconnects the session. The RR(P) SRE is contrary to the LLC2 specifications.
The workaround is to specify XTX=7 on the route.nlm. [CSCdp09295]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with the following message:

```
%CIP2-3-MSG: slot0 %SCI802-3-FATAL_ERROR: SST_ASSERT failure in ../cta802/ciptask.c @ 322 - !mxcb->mx_next
%CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
```

The assertion is intended to detect messages with 15 or more memory buffers (mbufs). There is no workaround. [CSCdp13245]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails when running CSNA. This problem occurs while processing the detection of idle subchannel conditions.
The workaround is to avoid creating idle subchannel conditions by not using the Z NET cancel command. Other possible workarounds include shutting down the router channel interface or removing the CSNA configuration statement before issuing the Z NET cancel command. [CSCdp31175]

- The Cisco Mainframe Channel Connection (CMCC) adapter deletes all the PUs associated with IP pool and fails with an error message 35. This problem occurs when a listen-point PU and another non-listen-point PU are configured with the same IP address and TCP port pair and the no listen command is issued. PUs that are not configured under the listen-point are deleted.

The workaround is to not configure a listen-point PU and another PU with the same IP address and TCP port pair. [CSCdp45166]

- Cisco Mainframe Channel Connection (CMCC) adapter configuration errors occur when the CIP microcode is upgraded from Version cip24-14 to cip24-15. The following error message occurs when attempting to delete an allocate logical unit (LU) pool statement:

```
dec 20 05:48:57 UTC: %CBUS-3-CIPCFGFAIL: Channel0/2: configuration command
TN3270S_LISTEN_POINT_PU_LU_POOL cmd 40 failed
```

There is no workaround. [CSCdp56576]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with error message 35 when the TN3270 server is shut down. This problem occurs when using CIP microcode Version cip24-15 or later.

There is no workaround. [CSCdp58083]

- When the TN3270 server statistics are displayed, a negative LU IN USE message appears. This is a cosmetic problem. Logical units (LUs) are still available to the clients as needed.

There is no workaround. [CSCdp69064]

- When an online insertion and removal (OIR) of an IP card is performed on a Cisco 7500 series router with a CIP, the following error messages are displayed:

```
*Jan 18 00:56:35: %OIR-6-REMCARD: Card removed from slot 1, interfaces disabled
*Jan 18 00:56:40: %CIP2-6-MSG: slot5 %SYSMGMT_RPC-6-STATECHANGE: System Management activated
*Jan 18 00:56:47: %CIP2-3-MSG: slot5 %LOVE-3-LOVELETTER: Error in love letter processing for port 0(0)
```

There is no workaround. [CSCdp75240]

- The TN3270 server logical unit (LU) Nailing feature fails in a subnetted IP address scheme. This problem occurs because the client addresses are not recognized.

The workaround is to configure the tn-parameter code codevalue command with a code value of 9. This workaround applies only if the client is capable of requesting a specific logical unit (LU) name. If the client does not specify an LU name, then an LU will be awarded based on the LU Nailing rules configured. [CSCdp58041]

---

**Open Caveats in Version 27.4/Resolved Caveats in Version 27.5**

This section describes possible unexpected behavior in Version 27.4. All the caveats listed in this section are resolved in Version 27.5.

- BADTIMER messages appear when running the TN3270 server. In this case, the messages appear because a TN3270 session is being negotiated or recently has been negotiated. The messages do not impact normal TN3270 server operations.

There is no workaround. [CSCdk21633]
The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent, depending upon the timing between receiving data from the client and the shutdown sequence.

This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode Releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later. The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

The TN3270 server configured for a direct, non-APPN connection sets the parallel transmission group (TG) supported bit on xid3 to byte = 15(bit 0 of XID3).

This setting is incorrect for a LEN node direct connect configuration and causes connection failure problems when connecting to the SNA Switch. The SNA Switch expects the device to negotiate a TG number, but the TN3270 server does not support this action. The TN3270 server must either negotiate a TG number or not configure a TG-capable bit setting.

The workaround is to configure the snasw port command with the conntype len keyword specified on the SNA Switch port to which the TN3270 server connects. The TN3270 server will no longer set the parallel TGs supported bit during the XID exchange for direct PUs. [CSCdm71315]

The user is unable to acquire specific logical units (LUs) when using TN3270E clients. This error occurs intermittently on one of the several configured PUs. This error occurs when the customer is running direct-connect PUs (no DLUR) and does not have the INCLUD0E=YES parameter set on the switched major node. This error occurs in CIP microcode Version cip21-14, but the affected PUs do not have LU pools defined.

There is no workaround. [CSCdm73361]

Data is lost on printer emulators. This problem occurs when the user is running the TN3270 server in an environment with small (768) RU sizes and low pacing values. The printer receives the first RU of data, but intermittently fails to receive the second. The TN3270 server received an EXPEDITED SHUTD command prior to receiving the last-in-chain RU. The shutdown process causes loss of data.

This fix adds a 10-second delay between receiving the shutdown command and responding to the shutdown command. This time window will allow any data that is in the queue to transmit before the shutdown procedure.

There is no workaround. [CSCdm80945]

CSNA devices fail with INOP messages during Interface Control Check (IFCC) status. This problem occurs when CLAW and CSNA are operating in high traffic conditions. It can occur in Cisco MultiPath Channel (CMPC) and SNA, also.

The workaround is to upgrade the Cisco Mainframe Channel Connection (CMCC) microcode or to restart the external communication adapter (XCA) nodes. [CSCdm88239]

A BIND REQUEST or SSCP-LU message is expected but not received from the host within 30 seconds from the start of an SSCP-LU session for the Cisco Mainframe Channel Connection (CMCC) adapter TN3270 server session. If the condition continues for another 2 minutes, the logical unit (LU) is declared bad and the following error message appears:

%TN3270S-1-NO_BIND_REQ_RCVD: No BIND REQ received on LU [chars].[dec], 120*ONESEC

This error and several others are logged as priority 1 (alert) messages in error reports. The priority level of the following error messages is now priority level 3:

NO_PSID_RSP_RCVD
NO_NTFY_AV_RSP_RCVD
NO_BIND_REQ_RCVD
NO_SDT_REQ_RCVD
NO_SDT_TMARK_RCVD
NO_UNBIND_TMARK_RCVD
NO_NTFY_UA_RSP_RCVD
NO_DYN_ACTLU_REQ_RCVD
NO_UNBIND_RSP_RCVD
NO_TERMSELF_RSP_RCVD

There is no workaround. [CSCdm94788]

- Support is added for the TCP/IP information vector (CV64). The CV64 carries TN3270 server clients IP address, TCP port number, and optionally the DNS name. The CV64 is sent inbound along with the NOTIFY(enable) and RSP(ACTLU) messages.

VTAM indicates whether it can receive the CV64 by setting a bit in the PU Capabilities vector (CV80) in the outbound ACTPU Request message. For DLUR PUs with all static LUs, the VTAM might not send the CV80 and the TN3270 server will not send the CV64.

If the parameter INCLUD0E=YES is coded for this PU in the switched major node, the VTAM will send CV80 and enable the TN3270 server to send the CV64. [CSCdp06211]

- The TN3270 server client fails when configuring printer logical units (LUs). This problem occurs when the two LU definitions required to configure the printer are set. One LU is nailed with the client IP address and the other is nailed with the client IP address of the printer. The TN2370 Server allocates the video client to the printer LU and then neither client works. This problem occurs in CIP microcode Releases cip24-10 through cip24-13 and later.

There is no workaround. [CSCdp06760]

- The TN3270 server or TN3270E client fails when it connects to the server, but does not specify the name of an logical unit (LU) to be obtained. This problem occurs in CIP microcode Version cip24-14 and later when a combination of DDDLU and nailed LUs are used.

The workaround is to code an lu-seed in the router on the PU, then connect to a TN3270E client configured with the correct LU name. [CSCdp09708]

- When an ICMP Host Unreachable packet is received by the TCP stack, it generates several soft errors before the error becomes permanent. The Offload select() returns readable to the soft errors. [CSCdp18373]

- The Cisco Mainframe Channel Connection (CMCC) adapter with the TN3270 server configured fails with fatal error 35. This problem occurs when attempting to clear the TN3270 configuration from the router. After entering the no tn3270-server command while in configuration mode on the virtual channel interface, the microcode reloads and all the interfaces flap. The CSNA devices are removed from the running configuration and must be reconfigured.

There is no workaround. [CSCdp24670]

- The printer emulators receive a -RSP sense 2005 message. The problem is caused by an emulator that sends data to the host after the BIND, but before the Start Data Traffic (SDT) processing is complete. This data is rejected from the host and the following -RSP sense 2005 message appears:

J*FKP4390E UNEXPECTED DATA RECEIVED.QUE.HELD.LU="LUname"

There is no workaround. [CSCdp30854]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails when running CSNA. This problem occurs while processing the detection of idle subchannel conditions.
The workaround is to avoid creating idle subchannel conditions by not using the Z NET cancel command. Other possible workarounds include shutting down the router channel interface or removing the CSNA configuration statement before issuing the Z NET cancel command. [CSCdp31175]

- The CLAW control link does not establish. This problem most likely occurs on a TPF system or on an IBM TCP/IP system. The problem occurs because the timing of the Halt Subchannel message related to the Start Subchannel message is off.
  
  The workaround is to stop and restart the CLAW driver causing the CLAW control link to synchronize again. [CSCdp32675]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with error message 35. This problem occurs when adding a second TN3270 server PU under the DLUR and when the CMCC adapter is offline.
  
  There is no workaround. [CSCdp43223]

- A print server with 10 logical units (LUs) fails to get 10 TNET connections with the TN3270 server. The tenth LU client receives a FIN message from the TN3270 server. The TN3270 server rejects the TNET message indicating Listen Closed on the PU. Additional attempts to connect to the tenth LU fail until the LU is reactivated or another LU is disconnected. The problem only occurs when the last ACTLU static LU is obtained by a client. It is standard practice for the TN3270 server to close the listen vector at this time; however, it should not close any connections that are being negotiated and have obtained LUs.
  
  The workaround is to add an additional 3 LUs to the VTAM switched major node, leaving the print server to request only 10 TNET connections. [CSCdp43253]

- The Cisco Mainframe Channel Connection (CMCC) adapter calculates a set buffer address (SBA) that is above the screen size. This problem occurs when connecting a 327802 client using a 3270 datastream. This causes the connected session to hang on the MSG0 screen.
  
  The workaround is to code the LUGROUP parameter with one of the following values: SSCPFM=USS3270 or SSCPFM=USS3270. [CSCdp46564]

- The Cisco Mainframe Channel Connection (CMCC) adapter configured for TCP/IP Offload fails with an error message 35. This problem occurs after a %MBUF-0-MFREEx2 message error. The problem occurs in rare circumstances when a socket request close() is issued on a TCP/IP server socket which has an outstanding accept() socket response on a BLOCKING socket. This problem also occurs in the same circumstances on a CMCC adapter configured for TPF Offload.
  
  There is no workaround. [CSCdp47885]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with error message 35. This problem occurs when the no client ip command is issued in listen point submode.
  
  There is no workaround. [CSCdp55519]

- The TN3270 server client does not connect when requesting a resource by name. This problem occurs because the ACTLU improperly truncates the logical unit (LU) name. This problem affects all DLUR configurations and direct-connect configurations when INCLUDE0E is specified in the Switched Major Node definitions.
  
  There is no workaround. [CSCdp54029]

**Open Caveats in Version 27.3/Resolved Caveats in Version 27.4**

This section describes possible unexpected behavior in Version 27.3. All the caveats listed in this section are resolved in Version 27.4.
OpenConnect has an informal extension to the Termtype in TN3270. When connecting through an OpenConnect TN3270 gateway, the client IP address is concatenated on the end with a percent (%) symbol.

The Cisco Mainframe Channel Connection (CMCC) TN3270 server does not use this client IP address for matching on logical unit (LU) nailing statements in the configuration. [CSCdj44584]

MSG10 data from one logical unit (LU) might be seen on an LU already in session. This problem occurs when the TN3270 server remote MAC address resides on a different physical adapter or in a different physical machine, such as a front-end processor (FEP).

The workaround is to make sure that the RMAC TN3270 server PU resides on the same Cisco Mainframe Channel Connection (CMCC) adapter as the TN3270 server. [CSCdm01837]

In a duplicate MAC environment, the CIP will continue to respond to a TEST command when the lines configured for the external communication adapter (XCA) are in use. This problem prevents other duplicate MAC adapters from responding to new requests.

The workaround is to configure the maximum LLC or threshold to equal the number of XCA lines configured. [CSCdm29597]

The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent depending upon the timing between receiving data from the client and the shutdown sequence.

This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode Releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later.

The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

The Cisco Mainframe Channel Connection (CMCC) adapter fails with fatal error 35 during the TN3270 server shutdown. This problem occurs because the TN3270 server PUs are not communicating with the host.

A workaround is available. Contact the Cisco TN3270 server development engineers for the interim fix. [CSCdm61159]

The TN3270 server running DLUR/DLUS fails with fatal error 35. This problem occurs because the TN3270 server tries to invoke a SendACTLURSP using a NULL object reference.
This fix adds a debug message to the log and marks the ACTLU as not processed.
There is no workaround. [CSCdm69186]

- The DLUR pipe between VTAM and the Cisco Mainframe Channel Connection (CMCC) adapter hangs. This problem occurs when a large number of TN3270 server TCP/IP requests (1000 per CMCC adapter) arrive at the same time.
  The workaround is to space out the TCP/IP requests. [CSCdm75120]

- When the Cisco Mainframe Channel Connection (CMCC) adapter is configured with a large number of offload sessions, the following error message occurs:
  
  `%CIP2-3-MSG: slot0 %OFFL-3-NOMEM2: Not enough memory to process socket requests, 0 open, 0 in holddown`

  The workaround is to increase memory. [CSCdm76552]

- The TN3270 server fails with the following error message:
  
  `%DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)`

  This error occurs when the TN3270 server is shut down while traffic is still transmitting. [CSCdm78261]

- The unbind/bind sequence in the response time logic during a transaction does not reset the sample. This error causes an invalid response time which might be extremely large, depending upon the timing of the transaction. This problem occurs when the unbind keep is configured when the next transaction completes.
  There is no workaround. [CSCdm82521]

- A select() message does not respond or times out when the peer closes the connection. This problem is more likely to occur when using TPF.
  The workaround is to delay the shutdown for 20 ms after the last send() message. [CSCdm85311]

- The TN3270 IND$FILE file transfer performs poorly if the RU size is smaller than the maximum transmission unit (MTU). This problem occurs because the Cisco TN3270 server uses the Nagle algorithm by default.
  The workaround is to set the RU size so that it is at least as big as the MTU on the file transfer path. [CSCdm86734]

- The TN3270 server overwrites 1 byte of a Read Partition Query (RPQ) response. The overwrite occurs because of a logic that was entered to capture a non-standard SYSREQ key sequence for non-TN3270E emulators.
  There is no workaround. [CSCdm88195]

- A TPF receive message fails to retrieve all the data. The problem occurs when the TPF client performs a shutdown-writing and then tries to receive the data.
  The workaround is to not perform the shutdown-writing. [CSCdm92713]

- A Cisco Mainframe Channel Connection (CMCC) file transfer hangs or the keyboard stops working. The problem occurs when the IND$FILE uses structured fields and buffers that are 2000 bytes or greater. The keyboard is restored using the TN3270 write command instead of the structured field.
  The workaround is to use buffers that are 2000 bytes or less or nonstructured fields (presentation space transfer). To enable the fix in CMCC Releases cip27-4 and greater and xcpa27-4 and greater, you must configure the TN3270 tn-parameter code codevalue command with a code value of 7. [CSCdm93990]
- The VTAM to VTAM communication for APPN and FID2 hangs. The non-LLC2 HPR traffic does not hang. This problem occurs when both VTAMs are attached to the CIP running the Cisco MultiPath Channel (CMPC) feature.

  There is no workaround. [CSCdp00921]

- The Cisco Mainframe Channel Connection (CMCC) displays the following error message:

  slot0: Fix this

  This error will not cause any serious problems.

  There is no workaround. [CSCdp04360]

- A 4-to-5 second delay occurs between the Cisco Mainframe Channel Connection (CMCC) connection to the server and the USSMSG10 screen display. This problem occurs only in CMCC trains cip24-x, cip27-x, and xcpa27-x.

  There is no workaround. [CSCdp06877]

- The Cisco Mainframe Channel Connection (CMCC) fails with error message 35. The problem occurs when the TN3270 server is using the logical unit (LU) Nailing feature with the older PU definition for the nailed LUs instead of the LU Pooling definition in CMCC branches cip24-x, cip27-x, and xcpa27-x. The following example shows the old PU without the LU Pooling definition:

  pu CISCO 04921002 157.2.196.101 token-adapter 31 24 rmac 4000.7206.0001
  client ip 157.2.0.0 255.255.255.0 lu 4 20

  The problem occurs when the client ip or no tn3270 server command is entered. The problem also can occur when the interface is shut down.

  There is no workaround. [CSCdp07729]

- A TCP/IP Offload select() for readability message indicates that there are no readable sockets in the descriptor list when in fact there are readable sockets available. This problem occurs when the TCP/IP connection fails while a select() for readability message is outstanding on the socket.

  There is no workaround. [CSCdp08103]

### Open Caveats in Version 27.2/Resolved Caveats in Version 27.3

This section describes possible unexpected behavior in Version 27.2. All the caveats listed in this section are resolved in Version 27.3.

- The TN3270 server session disconnects after 150 seconds when the LOGON APPLID is not entered. In this case, there is no unformatted system services table (USSTAB).

  There is no workaround. [CSCdk83774]

- Adding and removing PUs configured in TN3270 DLUR causes the Cisco Mainframe Channel Connection (CMCC) adapter to reload with fatal error 32. This failure occurs when a shutdown command is issued during high traffic periods on the server. The following messages appear immediately before the error:

  %CIP2-1-MSG: slot1 %TN3270S-1-RP_PU_CONFLICT: RP & CIP hold conflicting PU name("xxxxxxx") or index(92)
  %CBUS-3-CIPCFGFAIL: Channel1/2: configuration command TN3270S_DLUR_PU_NEW cmd 18 failed
  %CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=32)

  The workaround is to perform the shutdown when the server load is light. [CSCdk83807]
The CIP running TN3270 fails with fatal error 35 when a \texttt{shut} command is issued to the TN3270 server. This problem occurs when the \texttt{shut} command is issued and the TN3270 server is operating at high capacity. The workaround is to issue the \texttt{shut} command only after the client traffic terminates. [CSCdk87658]

If a CIP2 PCA (Bus and Tag) has an Altera FLEX chip (the large chip on the PCA daughter card) with a date code of 9601 or greater, the CIP will fail with parity errors shortly after the card is first installed. The date code on the PCA can be found only by looking for a code on the edge of the chip or the top heat sink area.

The workaround is to upgrade to the recommended CIP microcode version which corresponds to your Cisco IOS software. [CSCdm28629]

The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent depending upon the timing between receiving data from the client and the shutdown sequence.

This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later.

The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

The CIP running the TN3270 server receives DSI562I error messages on the NetView console. The messages indicate that in the activate physical unit (ACTPU) control vector 80, unsolicited network management vector transport (NMVT) request units are not allowed. The CIP TN3270 server still sends product-set identification (PSID) NMVT messages for VTAM PUs with only logical units (LUs).

There is no workaround.

To enable the fix in the cip24-13 microcode, the \texttt{maximum-lu} command must be added to the TN3270 server configuration file. [CSCdm36152]

The CIP VTAM session hangs at the VTAM message10 menu. This problem occurs when the user is at the VTAM message10 menu and hits multiple blank Enter keys, and when the inbound request unit on the SSCP-LU session is 256 bytes or greater.

There is no workaround. [CSCdm37663]

The CIP fails and causes a CBUS restart. Activating the VTAM external communication adapter (XCA) causes the CIP to fail with fatal error 35. Repeated restarts and reactivation of the XCA produces the same results. This problem occurs when running Cisco IOS Release 11.2(18)BC and CIP microcode Version cip24-11.

The workaround is to use Cisco IOS Release 11.2(16)BC and CIP microcode Version cip24-10. [CSCdm53220]

When the Attention (ATTN) key is pressed, the TN3270 client sends PA1 and ATTN messages. This problem occurs for IBM Personal Communication clients only.

To enable this fix and filter out the PA1 messages, you must configure the TN3270 \texttt{tn-parameter code codevalue} command with a code value of 2.

There is no workaround. [CSCdm54076]

Every other CIP TN3270 server client connection fails. This problem occurs when clients are trying to connect at a slow rate and the TN3270 server is operating with a light traffic load.

There is no workaround. [CSCdm55234]
• The following message appears on the Cisco Mainframe Channel Connection (CMCC) console:
  
  bad error-code 12 given

  This valid error code indicates a missing TERMSELF response. The code to log and format this specific error into a console message is missing.

  There is no workaround. [CSCdm55961]

• The downstream mini-EN/DLUR is unable to connect because it incorrectly calculates the lengths on the REGISTER general data stream (GDS). Shutting down and restarting exacerbates the problem.

  The workaround is to reload the Cisco Mainframe Channel Connection (CMCC) adapter after changing the DLUR configuration. [CSCdm56389]

• Attachmate clients loop when attempting to connect to the server. This problem occurs when the client is running Attachmate software Version 6.2, the autoreconnect feature is enabled, and invalid client names are configured.

  The workaround is to upgrade to Attachmate software Release 6.3. [CSCdm58334]

• The TN3270 server response time to the clients is slow (2 to 90 seconds). This problem occurs only if the clients are on a Token Ring or FDDI network and the server is on an Ethernet network. The problem occurs when there is a moderate to heavy load on the network.

  The problem occurs because the client network maximum segment size (MSS) is set to 4000 and the server network MSS is set to 1500. The Cisco Mainframe Channel Connection (CMCC) TCP stack attempts to increase the maximum transmission unit (MTU) from 1500 to 4000 every 10 minutes for each TCP connection. The Cisco IOS software sends only one or two ICMP messages per second; therefore, some TCP packets are dropped and must be retransmitted. The retransmission intervals increase exponentially and these intervals appear to the user as a delay in response time.

  To enable this fix in microcode Version cip22-39 and later, you must configure the TN3270 server `keepalive seconds` command with a value of 14444. To enable this fix in microcode Version cip27-3, xcpa27-3 and later, you must configure the TN3270 server `tn-parameter code codevalue value` command with a code value of 5. Value is the number of minutes between path MTU discovery retries. The default is 10 minutes. A value of 0 implies an infinite timer value.

  There is no workaround for other microcode versions. [CSCdm61803]

• The Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload server socket application hangs. This problem occurs because an accept() socket request blocks after the select() indicated that the server socket was READABLE. The accept() socket request should have returned a so_error condition or the socket ID of a new client socket. In TPF Offload environments, where a single select() might monitor multiple sockets, this problem can cause the application to hang on multiple server sockets if an accept() is issued from the same thread that processes the select() response.

  The workaround is to close and reopen the server socket by restarting the server application on the host. [CSCdm63283]

• The Cisco Mainframe Channel Connection (CMCC) TN3270 server fails with fatal error 35. This error occurs if the fix in CSCdm58334 has been applied.

  There is no workaround. [CSCdm69837]

• The TN3270 server sends an LIC message to the DLUS on a +RSP. This message causes the DLUS to send an unbind message with sense data 400B0000 and to shut down the DLUR/DLUS pipe. The DLUR/DLUS pipe will re-establish and the user LU-LU sessions will not be affected.

  This problem occurs when the TN3270 server DLUR component improperly saves RU chain bits from the original request to create a response message. This generates the +RSP sense data 400B0000.
The workaround is to increase the RU sizes on the DLUR/DLUS sessions. To increase the RU sizes on the DLUR/DLUS sessions, the user must do the following:

- Create a new member called ISTINCLM in the customizable datasets ahead of SYS1.VTAMLIB in the concatenation sequence for DD name VTAMLIB.
- Copy the ISTINCLM member from SYS1.SAMPLIB.
- Change the RU sizes in member CPSVRMGR from 0x9797 to 0xC8C8 and assemble and link.
- Issue the VTAM command
  FNET,TABLE,TYPE=MODETAB,OPTION=LOAD,NEWTAB=ISTINCLM
- Restart the TN3270 server DLUR end node. [CSCdm70432]

When the Cisco Mainframe Channel Connection (CMCC) adapter is configured with a large number of offload sessions, the following error message occurs:

%CIP2-3-MSG: slot0 %OFFL-3-NOMEM2: Not enough memory to process socket requests, 0 open, 0 in hold down

The workaround is to increase the memory. [CSCdm76552]

To enable the fix for CSCdk83774, the user must set the seconds value of the TN3270 keepalive seconds command to a multiple of 21. This prevents clients from disconnecting when the idle timer expires because there was not an SSCP screen.

To enable the CSCdk83774 fix in microcode Releases cip27-3, xcpa27-3 and later, you must configure the TN3270 tn-parameter code codevalue command with a code value of 6. [CSCdm76554]

Open Caveats in Version 27.1/Resolved Caveats in Version 27.2

This section describes possible unexpected behavior in Version 27.1. All the caveats listed in this section are resolved in Version 27.2.

- An Offload application uses up resources and prevents traffic from going through the port adapter on the Cisco Mainframe Channel Connection (CMCC). This occurs in very unusual circumstances only, for example, when closing several thousand established TCP connections in a very short period of time.

The workaround is to reload the CMCC microcode. [CSCdj08904]

- A VTAM connect out completion time greater than 20 seconds causes unexpected connection failures and external communication adapter (XCA) major node failures. This failure occurs because VTAM overloads the PORT TIMER and, if the PORT TIMER is set too low, the Link-State Advertisements (LSA). commands start to time out.

VTAM Version 4.3 introduced restrictions for the PORT TIMER value. The TIMER value cannot be less than the CMCC’s T1 * N2. VTAM uses a hard-coded N2 value of 2. Before this fix, the CMCC reported a T1 value of 10. The VTAM documentation indicates that the T1 value is measured in tenths of a second. Therefore, a T1 value of 10 should equal 1 second. However, VTAM interprets the T1 value in seconds so a T1 value of 10 equals 10 seconds, not 1 second. VTAM then multiplies the value by 2 to get a minimum TIMER value of 20 seconds.

The CMCC reported T1 value is not the CMCC LLC T1 value. Because VTAM overloads the use of the PORT TIMER, do not adjust the CMCC real LLC T1 value to alter the PORT TIMER. These adjustments can cause severe LLC2 problems.
VTAM overloads the use of PORT TIMER. TIMER is used to set TEST request interval on connect outs. After each TEST request is sent, VTAM sets a timer equal to the PORT TIMER number of seconds and waits for a TEST response. If the TEST response is not received by VTAM before the timer expires, the next TEST request is sent. In CMCC scenarios, the first TEST request is a TEST local, the second is a spanning-route explorer.

For the CMCC, most VTAM initiated LLC connections will not complete before the PORT TIMER seconds expire because the local TEST does not leave the CMCC internal LAN. LLC connection setup requires a minimum of 20 seconds. VTAM will timeout on LSA commands if a response is not received within the set PORT TIMER value. For example, when VTAM sends a CONNECT request the CONNECT CONFIRM must be received before the PORT TIMER expires. The SABME and UA must be exchanged within the value set in PORT TIMER. If the SABME must be retried, the PORT TIMERS might expire before the CONNECT CONFIRM is returned to VTAM.

The workaround is to set the PORT TIMER value to 20 seconds or more unless the user is confident that the LSA commands will not time out. [CSCdj45782]

When an online insertion and removal (OIR) of an IP card is performed on a Cisco 7500 series router with a CIP, the CIP processor utilization reaches maximum capacity (99 to 100 percent). This occurs when any IP card besides the CIP is inserted and removed online. If there are two CIPs in the router, an OIR of one CIP can affect the other.

The workaround is to not OIR IP cards in a Cisco 7500 series router when the CIP is running. [CSCdj90287]

The TN3270 server crashes with fatal error 35. See caveat CSCdk02535. [CSCdk11968]

During a brief TCP connection, the CMCC TCP/IP Offload feature fails to return a response to a Read/Recv type socket request, causing the connection’s host application to hang while waiting for a response.

A window exists for brief TCP connections when a connection is made with TCP/IP on the CMCC and then broken (FIN received) before Offload has received and processed an Accept socket request from the host. In this situation, Offload misses the notification from TCP/IP that the connection had been terminated.

There is no workaround. [CSCdk12291]

The TN3270 server session fails with the following error message:

```
INOP STATUS
```

The workaround is to reactivate the external communication adapter (XCA) major node. [CSCdk36329]

If a user disconnects without properly logging off the mainframe, a new user can connect to those existing sessions. This problem occurs when accessing Customer Information Control System (CICS) applications through the TN3270 server. [CSCdk48736]

Sometimes TN3270 client disconnections are counted twice. This miscount results in an incorrect TN3270 active session count. The dynamic logical unit (LU) count for that PU becomes one less than the actual number. This is not a problem until the actual count reaches zero and the dynamic LU count cycles to 255. When this miscount occurs, if you enter the `show extended ch4/2 tn` command, which shows how many LUs are in use, the result is inflated by 255.

The workaround is to shut down and restart the PU or to cycle the PU in VTAM. [CSCdk57112]

Inconsistent keepalives occur when multiple TN3270 sessions are configured to the same server. When the sessions are idle for an hour or more, keepalives are not sent, even though the keepalive value is set to 300 (5 minutes).

The workaround is to restart the session. [CSCdk57453]
- Dynamic logical units (LUs) remain in a P-NFT/UA state when the TN3270 server is configured. The LUs cannot be used again when in this state.

  The workaround is to deactivate the LU or the owning PU in VTAM. [CSCdk60263]

- The TN3270 session between the client and TN3270 server is disconnected when the client issues the `logoff` command at the VTAM MSG10 screen. [CSCdk80609]

- The TN3270 server session disconnects after 150 seconds when the LOGON APPLID is not entered. In this case, there is no unformatted system services table (USSTAB).

  There is no workaround. [CSCdk83774]

- When the TN3270 server is configured, entering the SYSREQ key followed by the `logoff` command does not return the user to the queued session. Instead, the VTAM MSG1 warning is displayed.

  Other SYSREQ key errors that occur when the TN3270 server is configured include:

  - Pressing the SYSREQ key twice does not return the user to the LU-LU session. An LUSTAT is sent inbound on the second SYSREQ key entry.

  - Entering the `logoff` command incorrectly locks the session. SSCP-LU does not recognize the change direction in a sense data frame. This problem might occur in other remote cases.

  - LU-LU data shows up on an SSCP-LU session.

  - When responding to DACTLU in LU-LU or bound states, an inbound unbind should be sent. This inbound unbind was not working, but it was not evident because the client is normally disconnected, which causes a SESSEND.

  The workaround is to not use the SYSREQ key. [CSCdk83960]

- The TN3270 server does not process the 0x016C6102 message from the client as a system request (SYSREQ). Therefore, the TN3270 server does not send a logoff message to the system services control point (SSCP). This message should produce the sequence described in RFC 1647 (TN3270E), except that 0x016C6102 is used to indicate SYSREQ instead of Abort Output (FFF5).

  There is no workaround. [CSCdk89383]

- CMCC devices with Bus and Tag connections do not activate properly when connected to an Amdahl 857 running the UTS operating system.

  There is no workaround. [CSCdk91964]

- For extended periods of time, the write device for a CLAW connection experiences the same number of command retries and connects. Data throughput decreases significantly during these periods, but the connection is not lost. The connections and the command retries are displayed with the `show extended channel slot/port` command. This situation occurs when the channel operates at 95 percent or greater capacity for many hours.

  A workaround is to distribute the traffic to multiple boxes to avoid a channel capacity of 95 percent or greater. [CSCdk92004]

- The CMCC TCP/IP Offload feature fails during select() processing when 28 or more sockets are defined in a single select request. If a select() request contains 28 or more socket descriptors in the descriptor list, the select() response is truncated after the offload message header. The mainframe offload application does not validate the offload message header buffer_length field and detect the ZERO length response data. Instead, it might process random data in the memory which follows the offload message header as the start of response data and incorrectly interpret the select() response results.

  This problem does not occur when using select() under VM or MVS because select() is issued for one socket at a time. This problem occurs when using TPF if the select() request contains 28 or more socket descriptors.
There is no workaround. This DDTS is a continuation of CSCdk86184. [CSCdm02126]

- If IP fragments that are 21 to 23 bytes long are sent to the CLAW of an OFFLOAD connection to a
  mainframe, the packet is dropped and the following error message is sent:

  CLAW-6-TOOSMALL: xx byte IP datagram is to small, device x/yyyy/zz

  The workaround is to modify the network so that IP fragments do not occur. [CSCdm11522]

- The CMCC unexpectedly reloads with the following error messages:

  %CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot 3, cmd code 2
  %CMCC-3-RSETFAIL: Interface Channel3/2: Error (8010) enable
  %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

  The problem occurs when the CMCC virtual interface is shut down or when a no tg hasas-ip or tg ip
  command is issued.

  There is no workaround. [CSCdm21378]

- If a CIP2 PCA (Bus and Tag) has an Altera FLEX chip (the large chip on the PCA daughter card)
  with a date code of 9601 or greater, the CIP will fail with parity errors shortly after the card is
  first installed. The date code on the PCA can be found only by looking for a code on the edge of the chip
  or the top heat sink area.

  The workaround is to upgrade to the recommended CIP microcode version which corresponds to
  your Cisco IOS software. [CSCdm28629]

- The TN3270 server session disconnects and brings up the Sign On menu. This problem occurs when
  a user has entered an AID command that it is queued in the server and then is scrolling through the
  session window. The server sends the AID to the host before receiving the end bracket specifying
  the direction.

  The following trace scenario illustrates the problem:

  - The BID command is received from the host:

    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: len=10,2C003601 00AE4B81 00C8
    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: sna-state=8501,lu-flags=0D24D204
    *Apr 26 13:36:24: %CIP: slot0 In Lu 5.54: len=10,2C000136 00AECEB8 00C8

  - An AID command is received before the host has a chance to send the BB command. Because
    the BID command was already received, the server queues the AID frame:

    *Apr 26 13:36:24: %CIP: slot0 In Tnet 212: len=13,00000100 42F7D7F5 11D7F5FF
    *Apr 26 13:36:24: slot0 Out Lu 5.54: sna-state=8D01,lu-flags=0D24D204

  - The host sends the next write with the BB/keyboard restored (note that there is no EB
    command):

    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: len=1484,2C003601 00AF0381
    80F10611 5D611DE8
    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: sna-state=8D01,lu-flags=0D24D204
    *Apr 26 13:36:24: %CIP: slot0 Out Tnet 212: len=1482,00000200 6C010411
    5D611DE8 40040404

  - The client sends the response to the frame:

    *Apr 26 13:36:24: %CIP: slot0 In Tnet 212: len=8,02000000 6C00FFEF
    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: sna-state=8509,lu-flags=0B24D204
    *Apr 26 13:36:24: %CIP: slot0 In Lu 5.54: len=9,2C000136 00AF8881 00

  - The BUG-inbound queued data was sent inbound before the EB command was received from the
    host:
There is no workaround. [CSCdm31347]

- The TN3270 server logical units (LUs) using LU Nailing fail. If a client IP address is nailed to an logical unit (LU) or range of LUs, then it cannot connect to the host. This problem occurs whether or not an LU name is supplied.

The following messages appear on the TN3270 console:

%CMCC: slot4 -----ient]0x40C:[connectReasonCode]0xE:[tn3270eDeviceType]IBM
%CMCC: slot4 -----3278-5-E:[tn3270eDeviceName]:[tn3270eSubErr]no-naill:

The workaround is to remove LU Nailing and restart the TN3270 server. Removing the LU Nailing command is not sufficient. Another workaround is to use a dynamic LU build. This build works with LU Nailing. [CSCdm36117]

Open Caveats in Version 27.0/Resolved Caveats in Version 27.1

This section describes possible unexpected behavior in Version 27.0. All the caveats listed in this section are resolved in Version 27.1.

- If the maxpiu value of the csna command is set to 4096 bytes, a CSNA-LONGREC error occurs when the sum of the size of an inbound frame and the size of the Link-State Advertisements (LSA). DataInd command exceeds 4 K. The CSNA-LONGREC error causes VTAM to terminate the connection.

The workaround is to increase the maxpiu value, preferably to the default, which is 20470 bytes. [CSCdk71668]

- The CMCC TCP/IP Offload feature fails during select() processing when more than 27 sockets are defined in a single select request. Failures include premature response to select requests, corrupt descriptor list in the select response, and the intermittent fatal error 32. These failures should only occur in Transaction Processing Facility (TPF) Offload environments.

The workaround is to limit the number of sockets selected in a single select request to 27 or less. [CSCdk86184]

- The CMCC unexpectedly reloads with the following error messages:

%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot 3, cmd code 2
%CMCC-3-RSETFAIL: Interface Channel3/2: Error (8010) enable
%DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

The problem occurs when the CMCC virtual interface is shut down or when a no tg hsas-ip or tg ip command is issued.

There is no workaround. [CSCdm21378]

Microcode Release 26 Caveats

This section describes the open and resolved caveats for microcode release cip26 and xcpa26. The caveats listed apply to only the most serious problems.
Open Caveats in Version 26.31/Resolved Caveats in Version 26.32

This section describes possible unexpected behavior in Version 26.31. All the caveats listed in this section are resolved in Version 26.32.

- The Tn3270 PU is in a WAIT state. The Virtual Channel Interface is in a Down/Down condition. Messages seen in the log:
  TN3270S-0-ILLEGAL_CCMUTEX_RELEASE: CIP2 slot1 : Releasing unacquired semaphore, lock held 800A9C4C lock_value FFFFFFFF ccMutex tcb 8010FCD0 thread tcb 81459CB0

  The Tn3270 PUs were hung and the Customer Shut/No Shut the Virtual Channel interface in an attempt to recover. The PUs would not recover.

  The workaround is to reload the CIP Microcode.

- The Tn3270 PUs in a WAIT state. The Virtual Channel Interface in a Down/Down condition. The following messages are seen in the log.
  TN3270S-0-ILLEGAL_CCMUTEX_RELEASE: CIP2 slot1 : Releasing unacquired semaphore, lock held 800A9C4C lock_value FFFFFFFF ccMutex tcb 8010FCD0 thread tcb 81459CB0

  The Tn3270 PUs were hung and the Customer Shut/No Shut the Virtual Channel interface in an attempt to recover. The PUs would not recover.

  The workaround is to reload the CIP Microcode.

- Part of the output of the Channel Interface Processor, CIP, console command tasks is misleading:
  CPU(1/5/60/busy): 1% 1% 0% 82%

  "Busy" includes time that will be used when there is other work to be done.

  The workaround is to disregard "busy".

- The TN3270-server DLUR controlled LU logon fails with either sense 80140003 or 087D0001. Topology on DLUS shows an ENDPT TG as OPER when in fact it is no longer operational.

  CIP/xCPA TN3270-server DLUR with multiple end point transmission groups (TGs). TN's DLUR name (CP name) must be greater in the collating sequence than the CP name of the DLUS.

  The workaround is to determine and delete the TG that is really not operational but is listed as operational on the DLUS host.

- A CIP/XCPA adapter configured for CSNA may run out of memory over time. You may see the following error message posted in the router log when the memory has been exhausted.
  %CIP2-6-MSG: slot0 %CTA-6-INACT_FREEMEM: Free Memory: 0x00090FE8
  %CIP2-6-MSG: slot0 %CTA-6-INACT_SLOWDOWN: Slowdown Rcvd: Yes, 180001 ms
  %CIP2-6-MSG: slot0 %CTA-6-INACT_SLOWDOWN: Slowdown Sent: Yes, 5089667 ms
  %CIP2-6-MSG: slot0 %CTA-6-INACT_SCBS: SCBs in SLC: 128
  %CIP2-6-MSG: slot0 %CTA-6-INACT_FLOW_COUNTS: Flow stop/resume 224/221
  %CIP2-6-MSG: slot0 %CTA-6-INACT_ATTNT_STATE: Attention FSM state: READ PENDING
  %CIP2-6-MSG: slot0 %CTA-6-INACT_FLOW_QUEUED: Flow Resume queued in CTA: 0
  %CIP2-6-MSG: slot0 %MSG802-6-FLOW_OFF_COUNT: On 505, Off<30 0, Off>30 0, total 505, max off time 0 ms
A buffer may be orphaned when an LLC2 session is terminated due to the T1 timer expiring N2 times. This issue was seen on CIP microcode 27-21.

The workaround is to issue a "microcode reload" command to free up the memory on the CIP/XCPA.

- In a Cisco 7500 router with a CIP2, the CIP2 may crash with a fatal error 32. The problem also may occur on a Cisco 7200 with an XCPA. The problem may occur when a channel interface with CSNA(s) is shutdown or when a CSNA is unconfigured.

There is no workaround.

- CIP microcode unexpectedly reloads with fatal error 35. This is a rare occurrence that can happen if a tn3270 client is disconnected during the processing of data to that client.

There is no workaround.

- %CIP2-6-MSG: slotx %ADAPTER-6-LOGOUT: ESCON dump output is followed by the %DEBUGGER-0-FATAL_ERROR: Fatal error (code=37) dump.

The write subchannel receives a HSCH or a CSCH while the read subchannel is waiting for access to the channel. This will only occur with very heavily utilized claw packing channels. This was observed with a feature of a mainframe TCP/IP stack that stopped and restarted a packed CLAW connection. The stack restarted the CLAW connection when there was no input from the CMCC.

The workaround is to avoid stopping packed CLAW links while there is traffic.

- The SCB limit on port NN reached, correlator: NNNN task: NAME XXXXXXXXX. might be seen for a Channel interface, CIP2 or XCPA. Many CSNA definitions are removed or shutdown.

The workaround is to reload the microcode on the interface.

Open Caveats in Version 26.30/Resolved Caveats in Version 26.31

This section describes possible unexpected behavior in Version 26.30. All the caveats listed in this section are resolved in Version 26.31.

- TCP connections for TN3270 clients might remain in the close-wait state indefinitely after a client disconnects.

This problem only occurs if the client happens to disconnect while the LU (logical unit) is in the state of waiting for ACTLU (activate LU). This might occur if the LU group major node is not active, or if ACTLU is slow to arrive. If the client reconnects, a new TCP connection would be opened while the old connection remains in close-wait. The new connection will operate normally.

There is no workaround. [CSCdx01730]


This section describes possible unexpected behavior in Version 26.29. All the caveats listed in this section are resolved in Version 26.30.

- Print jobs through an Open Connect print server are sometimes suspending.

This is occurring when the host application fails to send an End Bracket Indication (EBI) to the Secondary Logical Unit (SLU, which is the printer) prior to unbinding the session. The EBI triggers the TN3270 server to send IAC-Abort Output (AO) to the client that indicates the print job is complete. In the absence of EBI, the IAC-AO is not sent to the printer, and the print does not complete.
With the fix, the CMCC TN3270 server sends AO (Abort Output) to non-E printers or End of Job (EOJ) for E-printers when it is in receive state (in bracket in the outbound direction) when the TN3270 server receives an UNBIND. This will force data previously written to the printer to be printed.

There is no workaround. [CSCdp72090]

- When we inactivate an XCA major node in VTAM, VTAM has sent DACTPU commands and received DACTPU ACKs to/from all of the TN3270 server PUs. However, some TN3270 server PUs may not become inactive and subsequently cannot be activated. When this occurs, the TN3270 server PU status (shown using the `show extended channel tn3270-server` command) remains as “P-ACTPU” or “ACT-BUSY”.

The workaround is to run the `shut` and `noshut` commands at the PU scope, which properly activates any PUs that are suspended in this condition. [CSCea47302]

- If a CMPC connection from an OS host is inactivated by VTAM (the local major node PU is inactivated), then the router log reports the following message:

```
CIP2-3-MSG: slot5 %MPC-3-BAD_HDR: Unrecognized MPC header received: 0000C000 00000000
```

The CIP does not clear the LLC2 connection. Therefore, the upstream link remains connected. CMPC is not processing the DISCONTACT request from VTAM, so the LLCC (MPC LLC) connection is left in a bad state preventing the subsequent attempts to activate the LLC connection from completing.

This problem does not exist between the CIP and OS/390 systems.

The workaround is to reconfigure the connection using CSNA or CMPC+. [CSCea71612]


This section describes possible unexpected behavior in Version 26.28. All the caveats listed in this section are resolved in Version 26.29.

- The CIP or CPA interfaces that are configured for CLAW can get fatal error 37.

  The fatal error 37 can appear after the following messages:

  ```
  %%%BSQ-0-SCB_CHAIN: CIP2 slot4 : Read SCB chain is out of sequence
  or
  %%%ADAPTER-6-LOGOUT: CIP2 slotX : Port N logout data. Adapter microcode C50602D4
  ```

  The mainframe syslogs will show channel errors for the devices. The fix allows for additional error checking conditions so the ESCON code can recover and not take a fatal error.

  There is no workaround. [CSCdy06181]

- Unused Cisco Multi Path Channel Transmission Group (CMPC TG) connections might lead to a buffer shortage in the CIP or CPA. The result is that no CMPC TGs will be able to reconnect once disconnected. This has been observed on a CPA running xcpa26-26 microcode.

  The workaround is to disable the host PUs (physical units) associated with the CMPC TG to stop the buffer leak root cause, and then to issue a microcode reload to recover the lost buffers. Another workaround is to remove any unused CMPC TGs from the router configuration. [CSCdy44696]

- The CIP dumps with a fatal error 35 in RcvDACTxU.

  A DACTLU (deactivate LU) packet is being received to an LU (logical unit) that the DLUR application does not currently have defined. DLUR should be rejecting the DACTLU with sense 08120007 rather than crashing with a fatal error.
Caveats for CIP and CPA Microcode

- When using the NetSolve application on the mainframe to query the CIP for TN3270 LU names, you might see the LU name display as a blank or the LU name might be incomplete. The problem is only seen on applications that use the TN3270 Monitor interface to the CMCC TN3270 server. The workaround is to use the Cisco IOS `show extended channel tn3270-server` command to display LUs. [CSCdz15898]

- CCA-0-DEV_ERR2: Device error but no active defined device. The CIP or CPA crashes with DEBUGGER-0-FATAL_ERROR, unexpected reload with fatal error code=37. The CIP or CPA receives a frame from the host mainframe, but due to a logic error in the ESCON chipset on the CIP and CPA, it is not handled correctly. The CIP or CPA detects the logic error in the chipset and forces a microcode reload with a fatal error. There is no workaround. [CSCdz31806]

- The output from the `show extended channel tn3270-server pu` command displays the LU as inactive while the VTAM display from the command `d net,id=nnnnnnnnn,e` (where nnnnnnnn is the LU name) shows the LU as unstable. The client connects to the TN3270 server and TN3270 sends a Notify Available to VTAM. If the client disconnects while TN3270 is still waiting for the Notify response, and if the response is not received in a predefined timeout, the described symptom can occur. This is because TN3270 puts the LU in reset state without notifying VTAM. TN3270 now has the LU as being inactive while VTAM thinks it is active, but unstable. An attempt to inact/act the LU at this point results in the LU being stuck in the PDACL state in VTAM. There is no workaround. [CSCdz36410]

- The CIP TN3270 server advertises its MAX I-FIELD=4105 during XID negotiation even though the RIF indicates the MAX frame is 1500 bytes. When sending an XID, the value being reported for the maxIField (bytes 10-11 in XID) might be too large if the previously received RIF from a test packet indicates a lower value. The TN3270 server should be comparing its MaxIField from the SAP with the MaxDataRoute (received from the link-station partner via Test/RIF), and report the smaller of the two when sending the XID. There is no workaround. [CSCdz38697]

- Under certain circumstances when the TN3270 server is configured for DLUR, it can misinterpret the SLU name it receives if the PCID includes x4B in the received bind request. The LU-LU session is unbound with sense code 8004 0000. In this situation, the TN3270 server is configured as DLUR. The DLUS returns the returns the SLU name not network qualified. The PCID contains x4B. There is no workaround. [CSCdz48129]

- The status of the LU in VTAM is PSESEND-P, while the LU state on the router is ACT/NA. This problem can occur if a client is bound to an application, but has entered the SSCP session (via system request key) to make a request. In this case, the TN3270 server thinks that the client is waiting to be bound to some other application. If the client disconnects while in this state, the server goes into a “waiting for bind” condition and ignores a subsequent unbind (because the server incorrectly thinks that the LU is not currently bound). When VTAM receives no response to the unbind, the LU is placed into the PSESEND state. There is no workaround. Once the condition is observed you must cycle the LUs in VTAM. [CSCdz69040]
Open Caveats in Version 26.27/Resolved Caveats in Version 26.28

This section describes possible unexpected behavior in Version 26.27. All the caveats listed in this section are resolved in Version 26.28.

- CIP does not clean up properly after VTAM or an XCA major node is recycled. The following error messages appear in the router log:
  
  `6:43:13.323: %ECPA-6-MSG: slot1 %MSG802-6-LLC_DUP_CCB: LLC Station : RMAC=4000.4000.0002 LMAC=4000.4000.2222 LSAP=04 RSAP=C6`

  **Note** The following workaround might lead to a microcode reload, and should only be performed if a microcode reload is a tolerable side effect.

  The workaround is to issue a `shut` command followed by a `no shut` command while you are in TN3270 PU configuration mode. This seems to clear the PU condition, and it will then go to active status. [CSCdr90542]

- NO_BIND_REQ_RCVD error is being logged for an LU when no bind should be forthcoming.
  
  While a client is attempting connection, the connection might be broken (for example, due to NEGOT_TIME_EXPIRED). If this occurs while the server is in the state of waiting for an outbound ACTLU (activate logical unit), the server is not properly cleaning up on behalf of the LU (logical unit). When ACTLU is eventually received for the LU that the client was connecting to, the TN3270 server puts the LU in the P-BIND state even though the client has already been disconnected. After a timeout, the NO_BIND_REQ_RCVD message is logged. There are no harmful effects from this other than the NO_BIND_REQ_RCVD messages in the log.

  There is no workaround. [CSCdu63277]

- `%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]` messages

  The following messages might be seen:

  `%CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR: lu error [bad tnetSession pointer]:
  luname:72 pu:80F1A2A0_tnet:0
  %CIP2-1-MSG: slotx %TN3270S-1-LU_ERROR_INFO: LU info: Event 16 12 3 10 4 8 18 9
  18 4 8 18 17 14 20 1 ,state = 5,anaState = 1
  %CIP2-1-MSG: slot5 01, flag = D0`

  This can occur when a 3270 client has disconnected, and while the disconnect processing is occurring, an inactivity timer expires on the client, forcing the TN3270 server to try to disconnect the client which is already disconnected. This is a very small window and a very rare occurrence.

  The workaround is to disable configuration options that would cause clients to disconnect due to inactivity, such as `keepalive` and `idle-time`. [CSCdw31269]

- The TN3270 server does not send inbound notify or termself following a NO_BIND_REQ_RCVD error.

  This can occur while an LU is in the SSCP state (immediately following client connection or unbind/passive) and a bind is not received within a 2.5 minute timeout. The consequence is that VTAM/CICS does not clean up. Whatever application is currently assigned to the LU will remain, and the next client to connect might get an incorrect application.

  There is no workaround. [CSCdx56737]

- A NO_BIND_REQ_RCVD error is logged for TN3270 printers and the printers disconnect.
When a printer connects to the TN3270 server, but no print jobs are ready to be printed, the TN3270 server disconnects after 2.5 minutes and a NO_BIND_REQ_RCVD error is logged. If this occurs, subsequent printing fails because the printer is no longer connected.

The TN3270 server should not disconnect printers when a BIND is not received within 2.5 minutes. This should only occur for LU type 2 (display) clients.

The workaround is to verify whether print jobs are ready to be sent to the printer before connecting to the TN3270 server. [CSCdx58390]

- The CIP or CPA might crash with a fatal error 35 in Aluc_Start_SscpLu.
  This is a very rare occurrence due to a small timing window when a client might disconnect while some other event (host packet processing) is in progress. This could incorrectly leave the LU (logical unit) in the LU-LU session state, even though the client has disconnected. The result is that upon receiving subsequent packets (such as BIND, UNBIND), the server attempts to reference data structures that have been freed, resulting in the fatal error.

  There is no workaround. [CSCdy20175]

- LLC_DUP_SAP, fatal error 9 in ssi_buff.c, or PUs in P-ACTPU state due to a buffer loss condition.
  It is possible that other errors (such as ACT BUSY on PUs) could occur as a result of this buffer loss.

  The TN3270 buffers that are used to communicate to LLC layer are being lost, which eventually results in a depletion of the buffers and can cause any of the errors mentioned above. This buffer loss can occur during a link close or disconnect operation, such as would occur during a “shut” of TN3270, a listen-point or PU. A buffer is lost for each PU doing the close or disconnect operation.

  The buffer pool that is getting depleted is shown in the “tn3270 stats” (in the CIP or CPA console). The second line from the bottom of the stats output, is referred to as the “DLUR inbound pool free buffers.” The title is misleading as these buffers are also used for direct PUs.

  The following example shows the normal number of free buffers (150) in the DLUR inbound pool. When this buffer pool is low or depleted, the problems mentioned above can occur:

```
  Lstn Svcs inbound pool free buffers 520
  DLUR inbound pool free buffers 150 <=====
  DLUR outbound pool free buffers 520
```

  There is no workaround. [CSCdy46286]


This section describes possible unexpected behavior in Version 26.26. All the caveats listed in this section are resolved in Version 26.27.

- An AS/400 TN3270 client negotiates a termtype of IBM-3487 with the CIP TN3270 server. IBM-3487 is an invalid 3270 termtype and will not handle 3270 data streams correctly.

  This terminal type (along with similar models 3486, 3488, and 3489) should be rejected by the CIP.

  There is no workaround. [CSCdv83239]

- The CIP crashes with a fatal error code 35. Just before crash, the following error message type is logged:

```
bab LU on DISC: PU index is -1, LOCADDR is 216, DISC reason is 19
.remote IP address = 80.1.25.67, tnetSession = EE33BEAF, ipNext=0
&TN3270S_1-LU_ERROR: lu error [bad tnetSession pointer]:
  :216 pu:FF55DEAD, tnet:EE33BEAF
```
%TN3270S-1-LU_ERROR_INFO: LU info: Event 9 10 20 10 16 12 10 4 8 9 10 16 17 1 15

This error occurs after performing a “shut” on the TN3270 server. This could occur anytime the server attempts to disconnect a logical unit (LU) when the physical unit (PU) is in the process of being deleted.

There is no workaround. [CSCdr11739]


This section describes possible unexpected behavior in Version 26.25. All the caveats listed in this section are resolved in Version 26.26.

- A host receives an INOP 01 code message when a logical link control (LLC) session disconnects. This problem occurs when two Virtual Telecommunications Access Method (VTAM) systems are connected via an Advanced Peer to Peer Networking (APPN) network and an operation such as a Normal Disconnected Mode (NDM) file transfer is processed. One end of the connection terminates the operation normally. The other end detects the Logical Link Control (LLC) session disconnection and forwards a close_station_indication message with a code 7657 to VTAM. The code 7657 is translated as an abnormal disconnection sequence and causes VTAM to issue an IST1412I message with a return code 7657 and an INOP code 01.

The CIP should send a normal LLC disconnection sequence indication with a code 7656 instead. This sequence indication is illustrated in the following example:

Hosta--cip/csna-------dlsw------cip/csna----Hostb

<----------------appn----------------------->

There is no workaround. [CSCdp12204]

- The binds from the Network Node Server (NNS) are rejected with sense code 08150004, local form session identifier (LFSID) in use.

This problem only occurs with Dependent Logical Unit Requestor (DLUR) physical units (PUs). It then occurs when the link to the NNS goes down. For example, with a 3745 controller acting as the NNS, a customer can take the tic down on the 3745, or shut the CSNA channel to the host.

The TN3270 server Dependent Logical Unit Requestor (DLUR) link failure clean up results in a condition where the LFSID is still in use, causing future (i.e. when the link recovers) BINDs from the Network Node Server (NNS) control point to be rejected with sense code 08150004. This failure to clean up the LFSIDs causes internal DLUR PU processing to improperly shut down processing of the lost links. The result is that the TN3270 server does not recover the DLUR/DLUS pipe, and the TN3270 physical unit (PUs) fail to activate.

There is no workaround. [CSCdu01381]

- A CIP fatal error 35 occurs after a shutdown of the TN3270 server or of the Dependent Logical Unit Requestor (DLUR) component of the TN3270 server. This problem does not occur often, but when encountered it appears to be related to high volume networks where the TN Server and host are busy. In most instances, the TN Server will also log messages for the Physical Unit (PU) or Logical Unit (LU) stating it did not get a response from the host in 30 seconds.

The fatal error occurs after issuing a shut command from routernam(e(cfg-tn3270)# or routernam(e(tn3270-dlur)# modes.

There is no workaround. [CSCdu03050]

- An invalid management processor card (MPC) buffer from the mainframe causes a fatal error 35 on CIP.
There is no workaround. [CSCdu66303]

- The following router syslog message appears prior to a fatal error 9. Its cause is unknown.
  
  %ECPA-3-MSG: slot4 %CMPCGTG-3-LS_FSM_ERR: TG Name: P2US6092-Ls, Event ISlepIFlowStop, State SSstationOpen
  %XCPA-3-STATUS: bay [4] Fatal error detected (code=9)
  %ECPA-3-MSG: slot4 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/ls.C @ 339 - msgP

  There is no workaround. [CSCdv25071]

- The following message appears during Cisco SNA (CSNA) and Cisco Multipath Channel (CMPC) configuration sessions:
  
  %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./mpc/mpc.C @ 5793 - msgP

  There is no workaround. [CSCdv58096]

- The following message appears during Cisco SNA (CSNA) and Cisco Multipath Channel (CMPC) configuration sessions:
  
  %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./mpc/mpc.C @ 5793 - msgP

  There is no workaround. [CSCdv58115]

- At show ext cn/2 pu/lu, some DDDLU LU names appear blank if host applications send NULL SLU data in the bind.

  There is no workaround. [CSCdj90734]

- A Cisco router with CIP running TN3270 and Cisco SNA (CSNA) reloads with the following error messages:
  
  %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./cta802/dlu.c @ 437 - this && this->read_q && msg
  %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)

  There is no workaround. [CSCdv63166]

- Sense code 0812 0007 errors and/or error message 0897 are returned in response to an Activate LU (ACTLU).

  This is much more likely to occur when using the dynamic logical unit (LU) naming feature. The problem is experienced if the Virtual Telecommunications Access Method (VTAM) host is Initial Program Loaded (IPL) without reloading the router.

  The workaround is if you IPL the host, then also reload the router to clean up internal data structures. [CSCdv71737]

- The CIP router crashes with a fatal error 37 when the mainframe is configured for Open Shortest Path First (OSPF).

  There is no workaround. [CSCdv72227]


This section describes possible unexpected behavior in Version 26.24. All the caveats listed in this section are resolved in Version 26.25.

- The CIP might fail with a fatal error 35 in ccb802.c.

  There is no workaround. [CSCdu36395]
- Common Link Access to Workstation (CLAW) packing failed to initialize when using cip26-20 or above. There were no specific conditions for this bug. This problem was caused by CSCds32524 when it introduced a new flag bit that only affects the CLAW feature, however, the fix has not been incorporated into CLAW packing.
  There is no workaround. [CSCdu80489]

- Multiple console messages appear when performing a CIP reload.
  There is no workaround. [CSCdv04228]


This section describes possible unexpected behavior in Version 26.23. All the caveats listed in this section are resolved in Version 26.24.

- When a microcode reload occurs, the router log does not indicate what version of CIP microcode is being reloaded.
  There is no workaround. [CSCdt82371]

- The TN3270 server Dependent Logical Unit Requester (DLUR) link fails to activate when the remote MAC (RMAC) is an Advanced Peer-to-Peer Networking (APPN) port on the same router. The BIND is rejected with sense code 80040000.
  The workaround is to change the RMAC to point to an external communications adapter (XCA), and not the APPN port. [CSCdu19516]

- A router with ESCON CPA (ECPA) loses the Cisco Multipath Channel Transmission Group (CMPC TG) link and becomes inactive, for some unknown reason. The log displays the following:
  "%ECPA-3-MSG: slot4 %CMPCCTG-3-LS_FSM_ERR: TG Name: WMP1B   - Ls, Event IXidInd, State SConnected"
  The workaround is to perform a shut/no shut on the interface. [CSCdu0527]

- A CIP fatal error 35 appears when processing a configure-nack to an Inter Processor Communication (IPC) message.
  There is no workaround. [CSCdu40818]


This section describes possible unexpected behavior in Version 26.22. All the caveats listed in this section are resolved in Version 26.23.

- A fatal error 35 occurs from the CIP TN3270 server, when TNSessionDisConnect is the last entry in the trace.
  There is no workaround. [CSCdt24977]

- The TN3270 server is not cleaning up the logical unit (LU). The LU is being reallocated for another session, which then displays the previous login screen at the host. The router displays the following message in the above situation:
  %CIP2-3-MSG: slot4 %TN3270S-3-NO_BIND_REQ_RCVD: No BIND REQ received on LU xxx
  There is no workaround. [CSCdt84286]
If a particular logical partition (LPAR) on the mainframe (MF) hangs, it could cause a CIP adapter to hang and not pass traffic. This can occur when running CIP microcode Release 26-17. The CIP can hang, providing no diagnostic output to determine the condition that caused the hang.

The customer might see the following message when this occurs:

%IPC_RSP_CBUS-3-NOBUF: No more IPC memd buffers to transmit IPC message.

This problem was seen in the following environment:

CIP Release 26-17, Cisco IOS Release 12.0(9)

\[\text{Topo: MF-1 MF-2} \]
\[\text{| \ \ / \ |} \]
\[\text{| \ \ / \ |} \]
\[\text{| \ \ / \ |} \]
\[\text{Escon Dir1 Escon Dir2} \]
\[\text{| \ \ / \ |} \]
\[\text{CIP rtr1 CIP rtr2} \]

The CIP adapter in each CIP router hung when LPAR 4 in MF-1 hung.

The workaround is to issue a microcode reload command and/or reload the router. We had to issue the microcode reload command twice before it took effect. \[\text{[CSCdt86405]}\]


This section describes possible unexpected behavior in Version 26.21. All the caveats listed in this section are resolved in Version 26.22.

- The TN3270 server allows a client to access logical units (LUs) that are nailed to another IP address. This particular problem only occurs on the 26-x release train. Typically, it manifests itself when the customer has a configuration with either a large number of individual LUs nailed or a combination of individual LUs nailed and subnets nailed.

The workaround is to inactivate and activate the LU from the Virtual Telecommunications Access Method (VTAM) site. \[\text{[CSCds44646]}\]

- When the USS messages are too long, the TN3270 server does not suppress the Clear key. Instead, the TN3270 server sends it to the virtual telecommunications access method (VTAM). The VTAM answers with an error message. An inbound clear aid should be suppressed and a write with keyboard restore is sent back to the client.

The workaround is to code shorter USS messages in the USS table. \[\text{[CSCdt51737]}\]

- After a Dependent LU Requester (DLUR) physical unit (PU) is varied inactive and active again, the logical unit (LU) allocation algorithm is altered so that the LUs are no longer allocated properly on alternating PUs.

The normal allocation scheme allows dynamic LUs to be allocated from a PU until a given PU has two less free LUs than the next PU. Because the server does not free up LU resources when the DLUR PU is inactivated, these previously used LUs will be allocated first upon reactivation, regardless of the load-sharing algorithm. The TN Server always uses free LUs that have resources allocated before allocating resources for any new LUs. The real problem is that the server should be freeing up LU resources for LUs that are not in session when the DLUR PU is inactivated.

The workaround is a shut/no-shut on the PU, which frees up the inactive LUs. However, this is not necessary or recommended, since having the LUs allocated/inactive only affects the method of allocating dynamic LUs. \[\text{[CSCdt62248]}\]
Open Caveats in Version 26.20/Resolved Caveats in Version 26.21

This section describes possible unexpected behavior in Version 26.20. All the caveats listed in this section are resolved in Version 26.21.

- Bouncing transmission groups (TGs) for Cisco Multipath Channel Plus (CMPC+) frequently causes the CIP to restart with the following messages:

  01:40:03:%ECPA-0-MSG:slot5 %BSQ-0-SCB_CHAIN:Read SCB chain is out of sequence
  01:40:03:%ECPA-0-MSG:slot5 %DEBUGGER-0-FATAL_ERROR:Fatal error (code=37)

  This problem is found in cip27 releases.
  The workaround is not to activate, then deactivate TGs frequently when traffic is running from the CIP to the mainframe. [CSCdk87042]

- When installing a new Common Link Access to Workstation (CLAW) packing feature, packstat from the CIP console does not work correctly when ELPs exceed 16.
  There is no workaround. [CSCdt42288]

- When too many TCP connections to a TN3270 physical unit (PU) IP address destination port 65535 exist, the CIP processor crashes with the following messages:

  %CIP2-0-MSG: slot4 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35) 27 19:00:06:
  %CIP2-0-MSG: slot4
  %SCHED-0-NOPROCID: No process id available for process creation
  %CIP2-0-MSG: slot4 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

  There is no workaround. [CSCdt47389]

- After the channel has timed out on the CIP, the following output is given:
  Con should be N.

```
    odyssey#show extended channel 0/1 status
    Path: 0190   -- ESTABLISHED
    Dev  Connects  Retries  Cancels  Selective  System  Device  CU
    E0     13       0       0       0       2       0       0
    Blocks  Bytes  Dropped Blk Memd
    Dev-Lnk Read  Write  Read  Write  wait  Con
    E0-00   0       0       0       0       0       0       Y

    Last statistics 0 seconds old, next in 10 seconds
```

  The above occurs when the channel has timed out due to the host having been stopped (i.e., “v net, cancel”).
  There is no workaround. [CSCdt47430]


This section describes possible unexpected behavior in Version 26.19. All the caveats listed in this section are resolved in Version 26.20.

- The CIP restarts with a fatal error 35 when configuring Cisco Multipath Channel (CMPC) statements with alternating no shut. This occurs if the following sequence is pasted in interface mode:

```
    int ch2/1
        cmpp C040 72 TG0 READ
        no shut
        cmpp C040 73 TG0 WRITE
        no shut
```

Channel Interface Processor and Channel Port Adapter Microcode Release Note and Microcode Upgrade Requirements
**Caveats for CIP and CPA Microcode**

```cmpc C040 74 TGI READ```

The workaround is to issue the `no shut` command only once. [CSCdm39276]

- The Block Dropped on Read subchannel increases when trying to bring up a CLAW session while the other CLAW session is active, and the log displays the following message:

  ```
  %CIP2-6-MSG: slot5  $SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
  ```

  This condition occurs only if under the following circumstances:
  - The CIP is running out of System Control Board (SCB).
  - Only one CLAW device is configured or there is one device which was hit by large number of packets in a short period of time.
  - You are trying to bring up or tear down one more CLAW session. You should:
    1. Shutdown the interface.
    2. Perform a microcode reload.
    3. Confirm that all CLAW devices are configured.
    4. Perform a no shut.

  There is a hole in the `get_scb` function, where we allocate and release SCB in the same thread. Because the CIP allocates SCB for control messages using this function, there is a potential CIP lock when the CIP is hit by the above conditions.

  There is no workaround. [CSCds32524]

- When using VRN (Virtual Routing Node) to connect the TN3270 server to multiple hosts, the server attempts to create many dynamic links with the host, which fails, but uses up all its available dynamic link stations.

  There is no workaround. [CSCds50942]

- When issuing the `llc stat protocol all` command on the CIP console, a fatal error 35 occurs. If we issue `llc` commands without configuring any adapters, a fatal error 35 results.

  There is no workaround. [CSCdt10243]

- The TN3270 server sometimes awards a client a logical unit (LU) nailed with a shorter netmask over an LU nailed with a longer netmask. This situation occurs in the following two scenarios.

  In the first scenario, the user configures a new client nailing statement that has a longer netmask than an existing client nailing statement that covers the same client. If the client has been awarded LUs in the past from the shorter netmask, then newer client connections will be awarded the LUs from the shorter netmask first.

  In the second scenario, the configuration already contains two nailed client statements, one with a shorter netmask. If the client connects using different model types, occasionally the client is incorrectly awarded an LU from the nailing statement with the shorter netmask.

  Following is a sample configuration problem fix:

  ```
  tn3270-server
  idle-time 60
  keepalive 60
  dlur NETA.JIMK NETA.MVSD
  lsap token-adapter 1
  link HOSTMVSD rmac 4000.7500.7500
  pu PU1 11111111 10.100.1.1
  client ip 10.100.0.0 255.255.0.0 lu 224 225
  pu PU2 22222222 10.100.1.1
  ```
client ip 10.100.1.0 255.255.255.0 lu 113 114

Prior to this fix, a client with an IP address of 10.100.1.10 would sometimes get LU 224 or LU 225 before LU 113 or LU 114. The TN3270 server should always award a nailed LU with a longer netmask over an LU with a shorter netmask.

A temporary workaround is to perform a shut and no shut on the TN3270 server. [CSCdt18785]


This section describes possible unexpected behavior in Version 26.18. All the caveats listed in this section are resolved in Version 26.19.

- The CIP Logical Link Control (LLC) WwCountChanges counter from the `show extended channel slot/port llc statistics mac sap mac sap` command and the ConnectFail counter from the `show extended channel slot/port llc statistics` command are not incrementing correctly.

  There is no workaround. [CSCds29197]


This section describes possible unexpected behavior in Version 26.17. All the caveats listed in this section are resolved in Version 26.18.

- When the CIP receives many small packets in a very short period of time, the router freezes or locks up and receives these messages:

  %CIP2-6-MSG: slot5 %SCB-6-WAIT: SCB limit on port 0 reached, correlator: 0 task: CLAW read0/C700/00 8040CE10
  %CIP2-6-MSG: slot5 %SCB-6-RESUME: SCB on port 0 available,correlator: 0 task: CLAW read0/C700/00 8040CE10

  The workaround depends on customer network topology and configuration. [CSCdr85879]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with a fatal error 9 because a corrupted or runt MPOA Client (MPC) frame has been received.

  %CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/mpc.C @ 2049 - ssi_msg_length( bfrP) >= (sizeof( MpcFra
  %CIP2-3-MSG: slot0 meHdr) + frameSize)
  %CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)

  There is no workaround. [CSCds27703]

- The CIP Common Link Access to Workstation (CLAW) packing hangs. This problem happens when CIP CLAW packing received an IP packet which is bigger than negotiated CLAW frame size minus CLAW packed header size.

  A workaround is to configure IP Maximum Transmission Unit (MTU) where the size would be negotiated packet frame size (cross check with PROFILE TCPIP definition in the mainframe) minus 4, which is the packed header size. [CSCds24793]

- Once a logical unit (LU) is disconnected, the client cannot reconnect for 10 seconds. This happens when the TN Server, listen-point, or physical unit (PU) is configured for `lu deletion never`, which is the default value. After an LU disconnects, the server waits for 10 seconds for the host to respond to an inbound power-off product-set identification (PSID). However, when `lu-deletion` is set to “never,” no PSID request is sent inbound, so no host response will be received. The server leaves the LU in this wait state for 10 seconds before a subsequent client can connect.
The workaround is to configure as lu deletion always. This will force the power off PSID to be sent inbound. [CSCds28146]

- A fatal error 35 is received from the CIP TN3270 server. The server tries to send a -RSP to a Start Data Traffic (SDT), but the client disconnects while waiting for a timing mark before sending the response.

  The workaround is not to configure the timing mark under the TN3270 server scope. [CSCds31131]

- The CIP router configured for Cisco Multipath Channel (CMPC) crashes with the fatal error 9 below when a virtual CIP adapter is removed that is part of an active transmission group (TG).

  This problem has also been seen when a TG is coded using an adapter that is not currently defined.

%ECPA-3-MSG: slot3 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/clean.C @ 372 - elemP
%ECPA-0-MSG: slot3 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)

  The workaround is not to remove adapters for TGs without first inactivating the TG from the host system. When defining TGs, make sure all adapters are configured first. [CSCds32606]

- The CIP card configured for Cisco Multipath Channel (CMPC) hangs with the following messages:

%RSP-3-RESTART: interface Channel0/2, output stuck
%LINEPROTO-5-UPDOWN: Line protocol on Interface Channel0/2,changed state to down

  The problem can also be seen by performing a tasks command on the CIP console when the central processing unit (CPU) is at 100 percent. Both symptoms are triggered by adding new Cisco Multipath Channel Transmission Groups (CMPC TGs) or the flapping of existing TG(s).

  A potential workaround is to add new TG(s) only during a maintenance window and update the configuration immediately following a reload of the microcode. [CSCds41393]

- The CIP/CPA restarts with a fatal error 35 when a transmission group (TG) is configured with an adapter number that exceeds the limit of 18. This occurs in all CIP/CPA code levels.

  The workaround is not to exceed the limit of 18 adapters that can be associated with all TGs. [CSCds47000]

- The TN3270 client configured for VT100 ANSI terminal should not be able to negotiate a session with the TN3270 server. This terminal type will be added to the list of unsupported terminal types. There is no workaround. [CSCds51099]


This section describes possible unexpected behavior in Version 26.16. All the caveats listed in this section are resolved in Version 26.17.

- The CIP TN3270 server uses pooled logical units (LUs). The LUs are statically defined to virtual telecommunications access method (VTAM) and lu-deletion never and lu termination termself are coded. Clients attempting to connect are getting the following message:

  THIS TERMINAL HAS REQUESTED A RESOURCE NOT KNOWN ON THE TN3270 SERVER. THEREFORE, IT IS BEING PLACED INTO A HOLD STATE. PLEASE CONTACT YOUR HELP DESK FOR RESOLUTION OF THIS PROBLEM.
During the session termination process, the LUs are not always returned to the pool. The pool eventually runs out of LUs, which results in the above message. DDTS CSCdr41500 fixed a problem where the lu deletion never command would not get passed to the CIP by the Cisco IOS software, but the DDTS CSCdr41500 fix is a contributing cause to this problem.

A workaround is to enter the following command from the CIP/CPA console:

```
if-con cip_slot c
    tn3270 option nmvt_psid 0
    if-quit
```

This command will not live through a router reload or microcode reload. [CSCdr66536]

- A fatal error 35 crashes, with a shut on the interface, TN3270 server, or virtual interface.
  There is no workaround. [CSCdr73141]

- Issuing the tasks query command from the CIP console with the wrong process ID number causes a fatal error 32.
  There is no workaround. [CSCdr74632]

- The printer does not respond to data flow when the TN3270 server holds the keyboard restore until a change direction command is received. We have added two new options to allow new keyboard restore functionality.

  The following options are now available:
  - **tn-parameter code 7**—Enables functionality per CSCdm93990; the server does not manipulate keyboard restore on chained WSFs, for all type devices.
  - **tn-parameter code 11**—Server does not manipulate keyboard restore on WSF, Write, and E/W commands for printers only.
  - **tn-parameter code 12**—Server does not manipulate keyboard restore on WSF, Write, and E/W commands for displays only.

All three of the commands can be enabled to provide totally nonmanipulative keyboard restore data stream flow. Client: Attachments 6.4 and 6.5.

There is no workaround. [CSCdr93053]

- When running the offload feature on a Cisco 7500 series router with a CIP and IBM TPF mainframe, the following message is displayed:

  %CIP2-4-MSG: slot0 %OFFL-4-BADDESC: Socket descriptor 3 in request is bad: state DESC_Holddown compare 3 might be encountered

  This message is a warning to show that CIP receives an offload request command for a socket which is already closed or no longer exists. This message causes no negative impact to the network or the mainframe.

  There is no workaround. [CSCdr98652]

- The CIP TN3270 server might produce the message:

  %TN3270S-6-BADTIM: Bad timer operation(1),ra=8006AF14,funcPtr=0,oldFuncPtr=80B6E5AC

  The values for ra and oldFuncPtr might be different. This message can appear if the server is configured for lu deletion termself. Unless other problems are noted, the message might be ignored. This DDTS applies only to BADTIMER messages with operation(1).

  There is no workaround. [CSCds00674]
Caveats for CIP and CPA Microcode

- When using a CIP on a Cisco 7500 series router or a CPA card on a Cisco 7200 series router, the Cisco Mainframe Channel Connection (CMCC) might crash with a fatal error. This is seen only in rare situations when the free memory in the CMCC is either completely utilized or highly fragmented.
  
  A workaround is to increase the memory on the CMCC. [CSCds05651]

- A fatal error 35 occurs when removing the TN3270 server DLUR configuration on the shutdown virtual channel interface.
  
  There is no workaround. [CSCds14146]

- The CIP Common Link Access to Workstation (CLAW) packing hangs. This problem happens when CIP CLAW packing received an IP packet which is bigger than the negotiated CLAW frame size minus CLAW packed header size.
  
  A workaround is to configure IP Maximum Transmission Unit (MTU) where the size would be negotiated packet frame size (cross check with PROFILE TCPIP definition in the mainframe) minus 4 (the packed header size). [CSCds24793]

- Once a logical unit (LU) is disconnected, the client cannot reconnect for 10 seconds. This happens when the TN Server, listen-point, or physical unit (PU) is configured for `lu deletion never`, which is the default value. After an LU disconnects, the server waits for 10 seconds for the host to respond to an inbound power-off product-set identification (PSID). However, when `lu-deletion` is set to “never,” no PSID request is sent inbound, so no host response will be received. The server leaves the LU in this wait state for 10 seconds before a subsequent client can connect.
  
  The workaround is to configure as `lu deletion always`. This forces the power off PSID to be sent inbound. [CSCds28146]

Open Caveats in Version 26.15/Resolved Caveats in Version 26.16

This section describes possible unexpected behavior in Version 26.15. All the caveats listed in this section are resolved in Version 26.16.

- A fatal error 9 occurs in CIP microcode Release 26-8. The specific function that contributes to this is unknown.
  
  There is no workaround. [CSCdr07060]

- A fatal error 35 was received when attempting to run large numbers of sessions in a test lab environment. The specific failure occurs when no available memory exists to service a new session request. The fix checks an existing kernel routine to determine the available memory. If insufficient memory exists, client connections and unsolicited Activate LU (ACTLU) requests from the host will also be rejected will be rejected.
  
  There is no workaround for this bug. [CSCdr07326]

- After an IPL a Cisco Multipath Channel (CMPC) connection does not reactivate unless the virtual telecommunications access method (VTAM) Major Node is recycled. A `Z net, quick` was issued to VTAM.

  VTAM--CPA/7200--FR Relay DLSW---7513/CIP----VTAM

  The mainframe at the Cisco 7200 router site is IPLed (`VTAM z net quick`) and the CMPC connections show PCTD2 on this host. On the Cisco 7513 host they are PREQC.
  
  The workaround is to cycle the VTAM major node at the PCTD2 side. [CSCdr07387]

- A BADTIMER message appears when starting the TN3270 server. The messages do not impact normal TN3270 server operations.
There is no workaround. [CSCdr11353]

- RU length error, Systems Network Architecture (SNA) sense data 10020000, is issued by virtual telecommunications access method (VTAM). VTAM is receiving a positive bind response whereby data is missing from the end of the SNA. Interrogation of the data in the bind response shows that it is missing the SLU name. As a result, the host logical unit (LU) is marked unusable. While not every bind response is in error, this pattern will continue over a period of time, until such time that all host LUs are marked unusable. Additional investigation of the frame shows corruption of the data at the end of the packet. Subsequent efforts to capture documentation on the problem have revealed the same bytes for corrupted data, hex 3A through hex 3F followed by random data. Data corruption is the result of processing a spanning explorer frame from OS2PING.EXE (OS/2 workstation utility) with a 64 byte payload, hex 00 through hex 3F.

The workaround is not to run the OS2PING.EXE to the CIP MAC address. [CSCdr42284]

- A customer receives a fatal error 35 from the CIP during normal running conditions. No commands were being entered at the time.

A bug in the TN Server software allows for non-RFC compliant negotiation exchanges to occur. Some of these exchanges have the potential to cause a fatal error 35 in the TN Server code, due to a NULL pointer reference.

There is no workaround. [CSCdr64719]

- A Systems Network Architecture (SNA) PU5 to PU5 connection going through CIP routers does not always recover after an outage is experienced in the downstream network. This problem is usually seen when there is no autogen lines coded in the external communications adapter (XCA), which is typically done for PU5 to PU5 connections because the lines and PUs are hard coded.

This problem has also been seen with PU2.0 and PU2.1 connections. The symptom is you will not see the CIP respond to the incoming test poll.

A potential workaround is to recycle the XCAs after doubling or tripling the number of autogen lines. [CSCdr65638]

- An AS/400 TN3270 client negotiates a termtype of IBM-3486-BA with the CIP TN3270 server. IBM-3486-BA is an invalid 3270 termtype and will not handle 3270 data streams correctly. This fix adds IBM-3486-BA to the list of known invalid termtypes in the CIP TN3270 server. The CIP sends a WONT TERMTYPE message and allows the client to negotiate a valid termtype.

There is no workaround. [CSCdr65906]

- Occasionally, the Cisco Multipath Channel (CMPC) was not processing the **attach sap confirm** message properly when a local Systems Network Architecture (SNA) major node for a CMPC Transmission Group (TG) was activated. The following message appears:

  %CMPTG-3-LS_FSM_ERR: TG Name: MVSG2 -Ls, Event IXidInd, State SOpeningStation

  A CMPC TG gets stuck in the SOpeningStation

  The workaround is to deactivate and reactivate the local SNA major node. [CSCdr75344]

- Cisco Multipath Channel (CMPC) Transmission Groups (TGs) get stuck in the SAttachSapPending State mode. This occurs if multiple CMPC TGs share the same SAP on an adapter at time when only one TG will get the attachsap.cfm message. The other TGs will remain in the SAttachSapPending state and will not become active.

  The workaround is to inactivate and then reactivate the LS major modes for affected TGs. [CSCdr87920]

This section describes possible unexpected behavior in Version 26.14. All the caveats listed in this section are resolved in Version 26.15.

- When a parallel link that connects a Cisco TN3270 server to another server and carries the control point-to-control point sessions goes down, the Cisco TN3270 cannot establish a control point-to-control point session with any server.
  The workaround is to define alternate links to the same VTAM host only at the host end, or avoid multiple links to the same VTAM host. [CSCdp02702]
- The CMCC adapter fails with a fatal error 9.
  CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../ssi/ssi_buff.c 0
  1035 - msgP->m_next
  Jan 31 15:40:12: %CIP2-0-MSG: slot0 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=09)
  There is no workaround. [CSCdp84989]
- The Offload socket response on the transaction processing facility (TPF) is delayed by 10 seconds or more. This problem occurs when there is a lack of MEMD buffers on the channel interface on the Cisco 7500 series router for a prolonged length of time. This applies to the CIP only.
  There is no workaround. [CSCdr33661]
- The CMCC adapter fails with multiple fatal error 35. This problem occurs when running Cisco IOS Release 12.0(10) and CIP or CPA microcode Version 26-10 or later.
  There is no workaround. [CSCdr54396]


This section describes possible unexpected behavior in Version 26.13. All the caveats listed in this section are resolved in Version 26.14.

- A user receives another user session when both users are logged into the same applications owning region (AOR) in the Customer Information Control System and that AOR is manually cancelled.
  The workaround is to not disconnect a client during the logon process; that is, after requesting an application from the SSCP screen, but before establishing the LU-LU session with that application. [CSCdm51110]
- The following message appears on the CMCC console:
  bad error-code 12 given
  This valid error code indicates a missing TERMSELF response. The code to log and format this specific error into a console message is missing.
  There is no workaround. [CSCdm55961]
- The CMCC adapter fails with an error message 32. This problem occurs when the TN3270 server is configured and is using, or has used, the TN3270 monitor or a similar product.
  The workaround is to not configure the TN3270 monitor or a similar product. [CSCdp16086]
- The TN3270 server show pu command output is missing logical unit (LU) states. The missing states are displayed as P-RESET. This applies also to the LU state objects in the TN3270 server MIB.
  There is no workaround. [CSCdp51038]
• The CMCC adapter fails with fatal error 32. This problem occurs when approximately 25 or more DLUR links are configured. The reply buffer is too small to contain all of the Cross Domain Init vectors and the positive locate reply.

  The workaround is to configure fewer DLUR links. [CSCdp79125]

• The CMCC adapter fails with fatal error 32 and the following log message:

  %TN3270S-1-RP_PU_CONFLICT:RP & CIP hold conflicting PU name(XXXXX) or index(xxx)

  This problem occurs when multiple PUs are defined and the no pu command is issued to remove a PU that is not the last in the chain. The problem also might occur when DLUR is configured.

  The workaround is to remove the last PUs in the list first (also known as last in first out [LIFO] order). [CSCdp98933]

• The CMCC adapter might fail when the shutdown command is configured in TN3270 submode.

  There is no workaround. [CSCdp99538]

• The CMCC adapter configured for CSNA might not respond to a test poll. This problem occurs because there is a miscount of the available IBM VTAM external communications adapter (XCA) resources. Typically an XCA autogen parameter is configured to automatically generate lines and PUs. This is not required for PU5-to-PU4 or PU5-to-PU5 communications.

  The workaround is to recycle the XCA major node. [CSCdr03103]

• The CMCC adapter fails with the following fatal error 35:

  %CTA-0-INACTIVE: PA1 CTA 7C00-50 reset after being inactive for 180 seconds

  The workaround is to shut down the CSNA subchannel before shutting down VTAM. [CSCdr13804]

• When using the TN3270 server monitor or a similar product such as SOLVE:Netmaster for TCP/IP, the length of the message fragment field is reported incorrectly. The field length is reported as “18”. It should be reported as “20”. The message fragment field is defined as follows:

  struct {short PACKED(pktLength); short PACKED(len);
  unsigned char PACKED(bytes[16]);}

  This is a cosmetic failure and is present in all CIP and CPA microcode releases.

  There is no workaround. [CSCdr24412]

• VTAM issues a V NET,INACT,TYPE=GIVEBACK message. The control point-to-control point session moves to the other DLUS, but the DLUR pipe stops and restarts on the same host.

  There is no workaround. [CSCdr28173]


This section describes possible unexpected behavior in Version 26.12. All the caveats listed in this section are resolved in Version 26.13.

• Users are unable to start new CMCC sessions. The results of a show extended channel x/2 tn command show that some PUs are in an ACT/Busy state. The results of a VTAM display of the PU show that the PU is in an active state.

  The workaround is to reload the microcode. [CSCdm44279]

• The TN3270 server running on TPF returns the following error message:

  Offload time out
This problem occurs when the client establishes a connection to the server, issues a request, gets the response, and then closes the connection by sending a RST (reset) segment.

The server issues a read to the connection; the read message is blocked and returns with the error message. The read message should return with a 0 message, meaning that the connection was closed. This problem happens after one minute.

There is no workaround. [CSCdr05011]

- The CMCC adapter running CIP Offload returns the following error message:

  %CIP2-4-MSG: slot0 %OFFL-4-BADDESC: 0/9300/60 Socket descriptor 259 in request is bad:
  state DESC_Holddown compare 259

  This is a cosmetic problem that should not impact performance.

  There is no workaround. [CSCdp84965]

- The CMCC adapter running CIP Offload reloads with a fatal error 35. This problem occurs when too many Offload and CLAW statements are configured on the same interface. The process table is shared by two interfaces and cannot exceed 530 processes. Each Offload uses 4 processes. Each CLAW uses 2 processes. There are about 20 to 30 processes that are always running in addition to any Offload or CLAW configurations.

  The workaround is to configure fewer Offload and CLAW statements. [CSCdp85560]

- The CMCC adapter fails with fatal error 32. This problem occurs when changing the IP address of a loopback interface.

  There is no workaround. [CSCdp85890]


This section describes possible unexpected behavior in Version 26.11. All the caveats listed in this section are resolved in Version 26.12.

- BADTIMER messages appear when running the TN3270 server. In this case, the messages appear because a TN3270 session is being negotiated or recently has been negotiated. The messages do not impact normal TN3270 server operations.

  There is no workaround. [CSCdk21633]

- The CMCC adapter fails with a fatal error message 37. The following error messages appear:

  %CONFIG-3-WORKLEFT:Work pending on work queue when device terminated
  %DEBUGGER-0-FATAL_ERROR:Fatal error (code=37)

  There is no workaround. [CSCp54593]

- The CIP configured for CSNA crashes with the following error message:

  %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ./cta802/dlu.c Fatal error (09).

  There is no workaround. [CSCdm22660]

- In duplicate MAC environments, idle Systems Application Architecture (SAA) gateway sessions terminate. SAA gateways time out the route to the CMCC MAC address and send receive ready poll (RR(P)) single route explorer (SRE) messages to rediscover the route. The CMCC adapter is not in session and responds to the RR(P) messages with a disconnect mode final (DM(F)) message. The SAA gateway then disconnects the session. The RR(P) SRE is contrary to the LLC2 specifications.

  The workaround is to specify XTX=7 on the route.nlm. [CSCdp09295]

- The CMCC adapter fails with the following message:
Caveats for CIP and CPA Microcode

OL-1951-26


This section describes possible unexpected behavior in Version 26.10. All the caveats listed in this section are resolved in Version 26.11.

- The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent, depending upon the timing between receiving data from the client and the shutdown sequence.

This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later.

The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

- The following message appears on the Cisco Mainframe Channel Connection (CMCC) console:

bad error-code 12 given

This valid error code indicates a missing TERMSELF response. The code to log and format this specific error into a console message is missing.
Caveats for CIP and CPA Microcode

There is no workaround. [CSCdm55961]

- Cisco Systems Network Architecture (CSNA) devices fail with INOP messages during Interface Control Check (IFCC) status. This problem occurs when Common Link Access to Workstation (CLAW) and CSNA are operating in high traffic conditions. It can occur in Cisco MultiPath Channel (CMPC) and CSNA, also.

  The workaround is to upgrade the Cisco Mainframe Channel Connection (CMCC) microcode or to restart the external communication adapter (XCA) nodes. [CSCdm88239]

- A BIND REQUEST or SSCP-LU message is expected but not received from the host within 30 seconds from the start of an SSCP-LU session for the Cisco Mainframe Channel Connection (CMCC) adapter TN3270 server session. If the condition continues for another 2 minutes, the logical unit (LU) is declared bad and the following error message appears:

  %TN3270S-1-NO_BIND_REQ_RCVD: No BIND REQ received on LU [chars].[dec], 120*ONESEC

  This error and several others are logged as priority 1 (alert) messages in error reports. The priority level of the following error messages is now priority level 3:

  - NO_PSID_RSP_RCVD
  - NO_NTFY_AV_RSP_RCVD
  - NO_BIND_REQ_RCVD
  - NO_SDT_REQ_RCVD
  - NO_SDT_TMARK_RCVD
  - NO_UNBIND_TMARK_RCVD
  - NO_NTFY_UA_RSP_RCVD
  - NO_DYN_ACTLU_REQ_RCVD
  - NO_UNBIND_RSP_RCVD
  - NO_TERMSELF_RSP_RCVD

  A temporary workaround is simply to recycle the affected LU at the VTAM console. This puts the LU back into normal circulation. [CSCdm94788]

- When an ICMP Host Unreachable packet is received by the TCP stack, it generates several soft errors before the error becomes permanent. The Offload select() returns readable to the soft errors. There is no workaround. [CSCdp18373]

- The Cisco Mainframe Channel Connection (CMCC) adapter with the TN3270 server configured fails with a fatal error 35. This problem occurs when attempting to clear the TN3270 configuration from the router. After entering the no tn3270-server command while in configuration mode on the virtual channel interface, the microcode reloads and all the interfaces flap. The Cisco Systems Network Architecture (CSNA) devices are removed from the running configuration and must be reconfigured.

  There is no workaround. [CSCdp24670]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails when running Cisco Systems Network Architecture (CSNA). This problem occurs while processing the detection of idle subchannel conditions.

  The workaround is to avoid creating idle subchannel conditions by not using the Z NET cancel command. Other possible workarounds include shutting down the router channel interface or removing the CSNA configuration statement before issuing the Z NET cancel command. [CSCdp31175]

- The Common Link Access to Workstation (CLAW) control link does not establish. This problem most likely occurs on a TPF system or on an IBM TCP/IP system. The problem occurs because the timing of the Halt Subchannel message related to the Start Subchannel message is off.

  The workaround is to stop and restart the CLAW driver causing the CLAW control link to synchronize again. [CSCdp32675]
• The Cisco Mainframe Channel Connection (CMCC) adapter calculates a set buffer address (SBA) that is above the screen size. This problem occurs when connecting a 327802 client using a 3270 datastream. This causes the connected session to hang on the MSG0 screen.

  The workaround is to code the LUGROUP parameter with one of the following values: SSCPFM=USS3270 or SSCPFM=USS3270. [CSCdp46564]

• The Cisco Mainframe Channel Connection (CMCC) adapter configured for TCP/IP Offload fails with an error message 35. This problem occurs after a %MBUF-0-MFREEx2 message error. The problem occurs in rare circumstances when a socket request close() is issued on a TCP/IP server socket that has an outstanding accept() socket response on a BLOCKING socket. This problem also occurs in the same circumstances on a CMCC adapter configured for TPF Offload.

  There is no workaround. [CSCdp47885]


This section describes possible unexpected behavior in Version 26.9. All the caveats listed in this section are resolved in Version 26.10.

• OpenConnect has an informal extension to the Termtype in TN3270. When connecting through an OpenConnect TN3270 gateway, the client IP address is concatenated on the end with a percent (%) symbol.

  The Cisco Mainframe Channel Connection (CMCC) TN3270 server does not use this client IP address for matching on logical unit (LU) nailing statements in the configuration. [CSCdj44584]

• MSG10 data from one logical unit (LU) might be seen on an LU already in session. This problem occurs when the TN3270 server remote MAC address resides on a different physical adapter or in a different physical machine, such as a front-end processor (FEP).

  The workaround is to make sure that the RMAC TN3270 server PU resides on the same Cisco Mainframe Channel Connection (CMCC) adapter as the TN3270 server. [CSCdm01837]

• In a duplicate MAC environment, the CIP will continue to respond to a TEST command when the lines configured for the external communication adapter (XCA) are in use. This problem prevents other duplicate MAC adapters from responding to new requests.

  The workaround is to configure the maximum LLC or threshold to equal the number of XCA lines configured. [CSCdm29597]

• The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent, depending upon the timing between receiving data from the client and the shutdown sequence.

  This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later.

  The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

• The Cisco Mainframe Channel Connection (CMCC) displays a RSP sense 089F0004 message when processing a REQACTPU message. The problem occurs when the VARY command is entered for DLUR PUs that have multiple PATH statements. The problem occurs because the DLUR sends a message to the DLUS containing an FQPCID value which DLUS created on an earlier acquisition of the PU. The host processes the FQPCID message as invalid.

  The workaround is to remove the PATH statements. [CSCdm42103]
- Users are unable to start new Cisco Mainframe Channel Connection (CMCC) sessions. The results of a `show extended channel x/2 in` command indicate that some PUs are in an ACT/Busy state. The results of a VTAM display of the PU show that the PU is in an active state. The workaround is to reload the microcode. [CSCdm44279]

- A user receives another user session when both users are logged into the same applications owning region (AOR) in the Customer Information Control System and that AOR is manually cancelled. The workaround is to not disconnect a client during the logon process; that is, after requesting an application from the SSCP screen, but before establishing the LU-LU session with that application. [CSCdm51110]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails with a fatal error 35 during the TN3270 server shutdown. This problem occurs because the TN3270 server PUs are not communicating with the host. A workaround is available. Contact the Cisco TN3270 server development engineers for the interim fix. [CSCdm61159]

- The TN3270 server running DLUR/DLUS fails with a fatal error 35. This problem occurs because the TN3270 server tries to invoke a SendACTLURSP using a NULL object reference. This fix adds a debug message to the log and marks the ACTLU as not processed. There is no workaround. [CSCdm69186]

- The TN3270 server sends an LIC message to the DLUS on a +RSP. This message causes the DLUS to send an unbind message with sense data 400B0000 and to shut down the DLUR/DLUS pipe. The DLUR/DLUS pipe will re-establish and the user LU-LU sessions will not be affected. This problem occurs when the TN3270 server DLUR component improperly saves RU chain bits from the original request to create a response message. This generates the +RSP sense data 400B0000. The workaround is to increase the RU sizes on the DLUR/DLUS sessions. To increase the RU sizes on the DLUR/DLUS sessions, the user must do the following:
  - Create a new member called ISTINCLM in the customizable datasets ahead of SYS1.VTAMLIB in the concatenation sequence for DD name VTAMLIB.
  - Copy the ISTINCLM member from SYS1.SAMPLIB.
  - Change the RU sizes in member CPSVRMGR from 0x9797 to 0xC8C8 and assemble and link.
  - Issue the VTAM command `FNET,TABLE,TYPE=MODETAB,OPTION=LOAD,NEWTAB=ISTINCLM`
  - Restart the TN3270 server DLUR end node. [CSCdm70432]

- The DLUR pipe between VTAM and the Cisco Mainframe Channel Connection (CMCC) adapter hangs. This problem occurs when a large number of TN3270 server TCP/IP requests (1000 per CMCC adapter) arrive at the same time. The workaround is to space out the TCP/IP requests. [CSCdm75120]

- When the Cisco Mainframe Channel Connection (CMCC) adapter is configured with a large number of offload sessions, the following error message occurs: `%CIP2-3-MSG: slot0 %OFFL-3-NOMEM2: Not enough memory to process socket requests, 0 open, 0 in holddown`
  The workaround is to increase memory. [CSCdm76552]

- The TN3270 server fails with the following error message:
%DEBUGGER-0-FATAL_ERROR: Fatal error (code=35)

This error occurs when the TN3270 server is shut down while traffic is still transmitting. [CSCdm78261]

- The unbind/bind sequence in the response time logic during a transaction does not reset the sample. This error causes an invalid response time, which might be extremely large, depending upon the timing of the transaction. This problem occurs when the unbind keep is configured when the next transaction completes.

  There is no workaround. [CSCdm82521]

- A select() message does not respond or times out when the peer closes the connection. This problem is more likely to occur when using TPF.

  The workaround is to delay the shutdown for 20 ms after the last send() message. [CSCdm85311]

- The TN3270 IND$FILE file transfer performs poorly if the RU size is smaller than the maximum transmission unit (MTU). This problem occurs because the Cisco TN3270 server uses the Nagle algorithm by default.

  The workaround is to set the RU size so that it is at least as big as the MTU on the file transfer path. [CSCdm86734]

- The TN3270 server overwrites 1 byte of a Read Partition Query (RPQ) response. The overwrite occurs because of a logic that was entered to capture a non-standard SYSREQ key sequence for non-TN3270E emulators.

  There is no workaround. [CSCdm88195]

- A TPF receive message fails to retrieve all the data. The problem occurs when the TPF client performs a shutdown-writing and then tries to receive the data.

  The workaround is to not perform the shutdown-writing. [CSCdm92713]

- A Cisco Mainframe Channel Connection (CMCC) file transfer hangs or the keyboard stops working. The problem occurs when the IND$FILE uses structured fields and buffers that are 2000 bytes or greater. The keyboard is restored using the TN3270 write command instead of the structured field.

  The workaround is to use buffers that are 2000 bytes or less or nonstructured fields (presentation space transfer). To enable the fix in CMCC releases cip27-4 and greater and xcpa27-4 and greater, you must configure the TN3270 tn-parameter code codevalue command with a code value of 7. [CSCdm93990]

- The VTAM to VTAM communication for APPN and FID2 hangs. The non-LLC2 HPR traffic does not hang. This problem occurs when both VTAMs are attached to the CIP running the Cisco MultiPath Channel (CMPC) feature.

  There is no workaround. [CSCdp00921]

- A TCP/IP Offload select() for readability message indicates that there are no readable sockets in the descriptor list, when in fact there are readable sockets available. This problem occurs when the TCP/IP connection fails while a select() for readability message is outstanding on the socket.

  There is no workaround. [CSCdp08103]

**Open Caveats in Version 26.8/Resolved Caveats in Version 26.9**

This section describes possible unexpected behavior in Version 26.8. All the caveats listed in this section are resolved in Version 26.9.
• An Offload application uses up resources and prevents traffic from going through the port adapter on the Cisco Mainframe Channel Connection (CMCC). This occurs in very unusual circumstances only, for example, when closing several thousand established TCP connections in a very short period of time.

The workaround is to reload the CMCC microcode. [CSCdj08904]

• A VTAM connect out completion time greater than 20 seconds causes unexpected connection failures and external communication adapter (XCA) major node failures. This failure occurs because VTAM overloads the PORT TIMER and, if the PORT TIMER is set too low, the Link-State Advertisements (LSA) commands start to time out.

VTAM Version 4.3 introduced restrictions for the PORT TIMER value. The TIMER value cannot be less than the Cisco Mainframe Channel Connection (CMCC) T1 * N2. VTAM uses a hard-coded N2 value of 2. Before this fix, the CMCC reported a T1 value of 10. The VTAM documentation indicates that the T1 value is measured in tenths of a second. Therefore, a T1 value of 10 should equal 1 second. However, VTAM interprets the T1 value in seconds so a T1 value of 10 equals 10 seconds, not 1 second. VTAM then multiplies the value by 2 to get a minimum TIMER value of 20 seconds.

The CMCC’s reported T1 value is not the CMCC LLC T1 value. Because VTAM overloads the use of the PORT TIMER, do not adjust the CMCC’s real LLC T1 value to alter the PORT TIMER. These adjustments can cause severe LLC2 problems.

VTAM overloads the use of PORT TIMER. TIMER is used to set TEST request interval on connect outs. After each TEST request is sent, VTAM sets a timer equal to the PORT TIMER number of seconds and waits for a TEST response. If the TEST response is not received by VTAM before the timer expires, the next TEST request is sent. In CMCC scenarios, the first TEST request is a TEST local, the second is a spanning-route explorer.

For the CMCC, most VTAM initiated LLC connections will not complete before the PORT TIMER seconds expire because the local TEST does not leave the CMCC’s internal LAN. LLC connection setup requires a minimum of 20 seconds. VTAM will timeout on LSA commands if a response is not received within the set PORT TIMER value. For example, when VTAM sends a CONNECT request, the CONNECT CONFIRM must be received before the PORT TIMER expires. The SABME and UA must be exchanged within the value set in PORT TIMER. If the SABME must be retried, the PORT ITMER might expire before the CONNECT CONFIRM is returned to VTAM.

The workaround is to set the PORT TIMER value to 20 seconds or more unless the user is confident that the LSA commands will not time out. [CSCdj45782]

• When an online insertion and removal (OIR) of an IP card is performed on a Cisco 7500 series router with a CIP, the CIP processor utilization reaches maximum capacity (99 to 100 percent). This occurs when any IP card besides the CIP is inserted and removed online. If there are two CIPs in the router, an OIR of one CIP can affect the other.

The workaround is to not OIR IP cards in a Cisco 7500 series router when the CIP is running. [CSCdj90287]

• The TN3270 server crashes with a fatal error 35. See caveat CSCdk02535. During a brief TCP connection, the Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload feature fails to return a response to a Read/Recv type socket request causing the connection host application to hang while waiting for a response.

A window exists for brief TCP connections when a connection is made with TCP/IP on the CMCC and then broken (FIN received) before Offload has received and processed an Accept Socket request from the host. In this situation, Offload misses the notification from TCP/IP that the connection had been terminated.

There is no workaround. [CSCdk12291]

• The TN3270 server session fails with the following error message:
INOP STATUS

The workaround is to reactivate the external communication adapter (XCA) major node. [CSCdk36329]

- An error occurs when using the TN3270 server to establish a connection to an application residing on a Migration Data Host (MDH) using a virtual routing node connection network.

  If a prior connection to the MDH from the server does not exist, it might take several attempts to make a connection. Once the initial connection is made, all subsequent connections will work.

**Note**

IBM VTAM has opened an APAR for the 8002 sense portion of this problem. Users must get the APAR PTF from IBM to get MDH to work with the virtual routing node on the Cisco Mainframe Channel Connection (CMCC).

There is no workaround. [CSCdk37107]

- The user is unable to track, using Hot Standby Router Protocol (HSRP) or SNMP Traps, the channel interface on a Cisco 7200 series router with a CPA. The channel interface is always up/up even if the physical interface cable is not attached to the CPA.

  There is no workaround. The fix is to use a new channel interface configuration command, state-tracks-signal, which is valid only for the CPA. This command directs the CPA channel interface state to follow the physical signal value when the interface is in the no shut state. [CSCdk44052]

- If a user disconnects without properly logging off the mainframe, a new user can connect to those existing sessions. This problem occurs when accessing Customer Information Control System (CICS) applications through the TN3270 server. [CSCdk48736]

  Sometimes TN3270 client disconnections are counted twice. This miscount results in an incorrect TN3270 active session count. The dynamic logical unit (LU) count for that PU becomes one less than the actual number. This is not a problem until the actual count reaches zero and the dynamic LU count cycles to 255. When this miscount occurs, if you enter the `show extended ch4/2 tn` command, which shows how many LUs are in use, the result is inflated by 255.

  The workaround is to shut down and restart the PU or to cycle the PU in VTAM. [CSCdk57112]

- Inconsistent keepalives occur when multiple TN3270 sessions are configured to the same server. When the sessions are idle for an hour or more, keepalives are not sent even though the keepalive value is set to 300 (5 minutes).

  The workaround is to restart the session. [CSCdk57453]

- Dynamic logical units (LUs) remain in a P-NFT/UA state when the TN3270 server is configured. The LUs cannot be used again when in this state.

  The workaround is to deactivate the LU or the owning PU in VTAM. [CSCdk60263]

- The TN3270 session between the client and TN3270 server is disconnected when the client issues the logoff command at the VTAM MSG10 screen. [CSCdk80609]

- The TN3270 server session disconnects after 150 seconds when the LOGON APPLID is not entered. In this case, there is no unformatted system services table (USSTAB).

  There is no workaround. [CSCdk83774]

- Adding and removing PUs configured in TN3270 DLUR causes the CIP to reload with a fatal error 32. This failure occurs when a shutdown command is issued during high traffic periods on the server. The following messages appear immediately before the error:
%CIP2-1-MSG: slot1 %TN3270S-1-RP_PU_CONFLICT:RP & CIP hold conflicting PU name("xxxxxxx") or index(92)
Where "xxxxxxx" is the PU name.
%CBUS-3-CIPCFGFAIL: Channel1/2: configuration command TN3270S_DLUR_PU_NEW cmd 18 failed
%CIP2-0-MSG: slot1 %DEBUGGER-0-FATAL_ERROR: Fatal error (code=32)

The workaround is to perform the shutdown when the server load is light. [CSCdk83807]

- When the TN3270 server is configured, entering the SYSREQ key followed by the logoff command does not return the user to the queued session. Instead, the VTAM MSG1 warning is displayed.

Other SYSREQ key errors that occur when the TN3270 server is configured include:
- Pressing the SYSREQ key twice does not return the user to the LU-LU session. An LUSTAT is sent inbound on the second SYSREQ key entry.
- Entering the logoff command incorrectly locks the session. SSCP-LU does not recognize the change direction in a sense data frame. This problem might occur in other remote cases.
- LU-LU data shows up on an SSCP-LU session.
- When responding to DACTLU in LU-LU or bound states, an inbound unbind should be sent. This inbound unbind was not working, but it was not evident because the client is normally disconnected, which causes a SESEND.

The workaround is to not use the SYSREQ key. [CSCdk83960]

- The CIP running TN3270 fails with a fatal error 35 when a shut command is issued to the TN3270 server. This problem occurs when the shut command is issued and the TN3270 server is operating at high capacity.

The workaround is to issue the shut command only after the client traffic terminates. [CSCdk87658]

- The TN3270 server does not process the 0x016C6102 message from the client as a system request (SYSREQ). Therefore, the TN3270 server does not send a logoff message to the system services control point (SSCP). This message should produce the sequence described in RFC 1647 (TN3270E), except that 0x016C6102 is used to indicate SYSREQ instead of Abort Output (FFF5).

There is no workaround. [CSCdk89383]

- Cisco Mainframe Channel Connection (CMCC) devices with Bus and Tag connections do not activate properly when connected to an Amdahl 857 running the UTS operating system.

There is no workaround. [CSCdk91964]

- For extended periods of time, the write device for a Common Link Access to Workstation (CLAW) connection experiences the same number of command retries and connects. Data throughput decreases significantly during these periods, but the connection is not lost. The connections and the command retries are displayed with the show extended channel slot/port command. This situation occurs when the channel operates at 95 percent or greater capacity for many hours.

A workaround is to distribute the traffic to multiple boxes to avoid a channel capacity of 95 percent or greater. [CSCdk92004]

- The Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload feature fails during select() processing when 28 or more sockets are defined in a single select request. If a select() request contains 28 or more socket descriptors in the descriptor list, the select() response is truncated after the offload message header. If the mainframe offload application does not validate the offload message header buffer_length field and detect the ZERO length response data, it might process random data in the memory which follows the offload message header as the start of response data and incorrectly interprets the select() response results.
This problem does not occur when using select() under VM or MVS because select() is issued for one socket at a time. This problem occurs when using TPF if the select() request contains 28 or more socket descriptors.

There is no workaround. This DDTS is a continuation of CSCdk86184. [CSCdm02126]

- A query on the snaLuOperSnaName field in the SNA-NAU MIB returns an unexpected value. The MIB query returns the administrative name instead of the SNA name. This problem occurs if a direct PU, not a DLUR, has an LUSEED defined. Direct PUs do not support DDDLU. Also, this problem occurs when the INCLUD0E = YES field is not specified on the switched major node (SWM).

The workaround is to use DLUR or DDDLU, or to specify the INCLUD0E = YES field on the SWM. [CSCdm13637]

- If IP fragments that are 21 to 23 bytes long are sent to the Common Link Access to Workstation (CLAW) of an OFFLOAD connection to a mainframe, the packet is dropped and the following error message is sent:

  CLAW-6-TOOSMALL: xx byte IP datagram is too small, device x/yyyy/zz

The workaround is to modify the network so that IP fragments do not occur. [CSCdm11522]

- CIP response times and utilization increase when a large number of TN3270 server connection attempts are made to the same source IP address. A large number of TCP no-op (NOP) messages are sent by the TN3270 server to the clients.

The fix limits the number of NOP messages sent to the clients. No configuration is required to enable the fix.

There is no workaround. [CSCdm23252]

- If a CIP2 PCA (Bus and Tag) has an Altera FLEX chip (the large chip on the PCA daughter card) with a date code of 9601 or greater, the CIP will fail with parity errors shortly after the card is first installed. The date code on the PCA can be found only by looking for a code on the edge of the chip or the top heat sink area.

The workaround is to upgrade to the recommended CIP microcode version which corresponds to your Cisco IOS software. [CSCdm28629]

- The TN3270 server session disconnects and brings up the Sign On menu. This problem occurs when a user has entered an AID command that it is queued in the server and then is scrolling through the session window. The server sends the AID to the host before receiving the end bracket specifying the direction.

The following trace scenario illustrates the problem:

  - The BID command is received from the host:

    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: len=10,2C003601 00AB4B81 00C8
    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: sna-state=8501,lu-flags=0D24D204
    *Apr 26 13:36:24: %CIP: slot0 In Lu 5.54: len=10,2C000136 00AECB81 00C8

  - An AID command is received before the host has a chance to send the BB command. Because the BID command was already received, the server queues the AID frame:

    *Apr 26 13:36:24: %CIP: slot0 In Tnet 212: len=13,00000100 42F7D7F5 11D7F5EF
    *Apr 26 13:36:24: slot0 Out Lu 5.54: sna-state=8D01,lu-flags=0D24D204

  - The host sends the next write with the BB/keyboard restored (note that there is no EB command):

    *Apr 26 13:36:24: %CIP: slot0 Out Lu 5.54: len=1484,2C003601 00AF0381 80F10611 5D61DE8
Caveats for CIP and CPA Microcode

- The client sends the response to the frame:
  *Apr 26 13:36:24:  %CIP: slot0 Out Lu 5.54: sna-state=8D01,lu-flags=0D24D204
  *Apr 26 13:36:24:  %CIP: slot0 Out Tnet 212: len=1482,00000200 6C010411 5D611DE8 40404040

- The BUG-inbound queued data was sent inbound before the EB command was received from the host:
  *Apr 26 13:36:24:  %CIP: slot0 Out Lu 5.54: len=9,2C003601 00B00391 40
  *Apr 26 13:36:24:  %CIP: slot0 In Tnet 212: len=8,02000000 6C00FFEF
  *Apr 26 13:36:24:  %CIP: slot0 Out Lu 5.54: len=9,2C0003136 00200392 20F7D7F5 11D7F5

There is no workaround. [CSCdm31347]

- The TN3270 server fails intermittently during the shutdown procedure. This failure occurs when the shutdown procedure is performed and TN3270 server sessions are receiving client data. The TN3270 server shutdown procedure sequence shuts down the TCP/IP stack prematurely. The failure is intermittent, depending upon the timing between receiving data from the client and the shutdown sequence.
  This problem occurs in Cisco Mainframe Channel Connection (CMCC) microcode releases cip22-35, cip24-10, cip25-10, cip26-5, xcpa 26-5, cip27-0, xcpa27-0, and later.
  The workaround is to perform the shutdown procedure when there is no activity on the TN3270 sessions. [CSCdm35562]

- The CIP running the TN3270 server receives DSI562I error messages on the NetView console. The messages indicate that in the activate physical unit (ACTPU) control vector 80, unsolicited network management vector transport (NMVT) request units are not allowed. The CIP TN3270 server still sends product-set identification (PSID) NMVT messages for VTAM PUs with only logical units (LUs).
  There is no workaround.

To enable the fix in the cip24-13 microcode, the maximum-lu command must be added to the TN3270 server configuration file. [CSCdm36152]

- The CIP VTAM session hangs at the VTAM message10 menu. This problem occurs when the user is at the VTAM message10 menu and hits multiple blank Enter keys and when the inbound request unit on the SSCP-LU session is 256 bytes or greater.
  There is no workaround. [CSCdm37663]

- Every other CIP TN3270 server client connection fails. This problem occurs when clients are trying to connect at a slow rate and the TN3270 server is operating with a light traffic load.
  There is no workaround. [CSCdm55234]

- The Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload server socket application hangs. This problem occurs because an accept() socket request blocks after the select() indicated that the server socket was READABLE. The accept() socket request should have returned a so_error condition or the socket ID of a new client socket. In TPF Offload environments, where a single select() might monitor multiple sockets, this problem can cause the application to hang on multiple server sockets if an accept() is issued from the same thread that processes the select() response.
  The workaround is to close and reopen the server socket by restarting the server application on the host. [CSCdm63283]
### Open Caveats in Version 26.7/Resolved Caveats in Version 26.8

This section describes possible unexpected behavior in Version 26.7. All the caveats listed in this section are resolved in Version 26.8.

- The TN3270 server crashes with a fatal error 35. See caveat CSCdk02535. [CSCdk11968]
- If a CIP2 PCA (Bus and Tag) has an Altera FLEX chip (the large chip on the PCA daughter card) with a date code of 9601 or greater, the CIP will fail with parity errors shortly after the card is first installed. The date code on the PCA can be found only by looking for a code on the edge of the chip or the top heat sink area.

The workaround is to upgrade to the recommended CIP microcode version which corresponds to your Cisco IOS software. [CSCdm28629]


This section describes possible unexpected behavior in Version 26.5. All the caveats listed in this section are resolved in Version 26.7.

- If the `maxpiu` value of the `csna` command is set to 4096 bytes, a CSNA-LONGREC error occurs when the sum of the size of an inbound frame and the size of the Link-State Advertisements (LSA) `DataInd` command exceeds 4 K. The CSNA-LONGREC error causes VTAM to terminate the connection.

The workaround is to increase the `maxpiu` value, preferably to the default, which is 20470 bytes. [CSCdk71668]

- The Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload feature fails during `select()` processing when more than 27 sockets are defined in a single select request. Failures include premature response to select requests, corrupt descriptor list in the select response, and intermittent fatal error 32. These failures should only occur in Transaction Processing Facility (TPF) Offload environments.

The workaround is to limit the number of sockets selected in a single select request to 27 or less. [CSCdk86184]

- The Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload feature fails during `select()` processing when 28 or more sockets are defined in a single select request. If a `select()` request contains 28 or more socket descriptors in the descriptor list, the `select()` response is truncated after the offload message header. If the mainframe offload application does not validate the offload message header buffer_length field and detect the ZERO length response data, it might process random data in the memory which follows the offload message header as the start of response data and incorrectly interprets the `select()` response results.

This problem does not occur when using `select()` under VM or MVS because `select()` is issued for one socket at a time. This problem occurs when using TPF if the `select()` request contains 28 or more socket descriptors.

There is no workaround. This DDTS is a continuation of CSCdk86184. [CSCdm02126]

This section describes possible unexpected behavior in Version 26.4. All the caveats listed in this section are resolved in Version 26.5.

- Certain ESCON conditions lead to LOGDATA error messages that result in a fatal error. The fatal error dump can cause the LOGDATA error messages to be lost. The lost LOGDATA messages contain critical information needed to determine the cause of the problems. The fatal error information usually contains secondary information about the problem.

  A workaround is to use the CIP core dump feature that is available in Cisco IOS Release 11.2BC and later. This feature saves all CIP memory to a file on an FTP server. The missing LOGDATA can be extracted from the core dump file. The workaround applies only for the CIP. [CSCdj61710]

- A print job hangs when printing through the Cisco Mainframe Channel Connection (CMCC) TN3270 server. The host application sends an exception response on the end bracket chain followed by a CHASE.

  There is no workaround. [CSCdk27199]

- The AS/400 TN client attempts to establish an IBM-3180-2 terminal-type session with a TN5250 terminal. If a session is not available, the AS/400 TN client automatically switches to the TN3270 with a 3270 terminal type. The AS/400 TN client receives an ACK message from the 3180 terminal type when expecting a 5250 datastream. Instead, the TN3270 server sends it a 3270 datastream. Because the Cisco Mainframe Channel Connection (CMCC) TN3270 server accepts the IBM-3180-2 terminal-type, the client does not switch to TN3270. [CSCdk37980]

- The OFFL-3-NOMEM2 and OFFL-3-REJSOCK error messages indicate the same problem and should be combined into one message called OFFL-3-NOMEMSOCK. [CSCdk39425]

- The Cisco Mainframe Channel Connection (CMCC) crashes with fatal error 37 after the BSQ-0-S CB_CHAIN: Read SCB chain is out of sequence. If the routing processor sends an IP packet to the CMCC for a Common Link Access to Workstation (CLAW)-type device and that IP packet header indicates a 0 byte packet, the CMCC incorrectly tries to send a 0 byte message to the host and eventually causes a FATAL_ERROR on the CMCC.

  There is no workaround. [CSCdk41469]

- LLC_DUP_CCB error messages appear on the router console. This problem occurs when multiple remote stations are configured with the same local MAC or SAP. The following is a sample configuration:

```plaintext
interface Channel2/2
no ip address
no keepalive
lan TokenRing 2
    source-bridge 102 1 400
    adapter 2 4000.8001.0102
tg PAN12  llc token-adapter 2 10 rmac 4000.9000.beef
tg PAN2  llc token-adapter 2 10 rmac 4000.8000.beef
```

  The error occurs if PAN2 is in the LocatingRemoteLinkStation state and the local SNA associated with PAN2 is deactivated and then reactivated.

  Possible workarounds include reconfiguring the router not to use the same local MAC or SAP, or deactivating then reactivating all local SNA nodes associated with that local MAC or SAP. Another workaround is to reload the microcode on the Cisco Mainframe Channel Connection (CMCC) having the problem. [CSCdk41506]
• The Cisco Mainframe Channel Connection (CMCC) adapter crashes with a fatal error 35 when reconfiguring an offload statement using the same IP address that was used in a previously configured offload connection. This error occurs if the CMCC adapter has not completed deconfiguration cleanup of the previous offload statement before the new offload statement is configured using the same IP address. For example, the current configuration is as follows:

```
offload e200 50 80.11.198.2 ciscovm rispix tcpip tcpip tcpip api
```

Reconfigure the offload statement as follows:

```
no offload e200 50 80.11.198.2 ciscovm rispix tcpip tcpip tcpip api
offload e100 52 80.11.198.2 ciscovm rispix tcpip tcpip tcpip api
```

To workaround, after deconfiguring the offload statement, exit the configuration and issue the `show extended channel slot/port ip-stack ip address` command. When the offload deconfiguration is complete for the indicated offload statement IP address, the output should indicate “...No IP statistics found”. At this point the new offload statement using the same IP address can be configured.

The following is an example configuration:

```
rispix#show ext ch 0/1 ip-stack
IP Statistics for IP Address 80.11.198.2
 Forwarding : no  DefaultTTL : 64  InReceives : 0
 InHdrErrors : 0  InAddrErrors : 0  ForwDatagrams: 0
InUnknownProtos: 0  InDiscards : 0  InDelivers : 0
OutRequests : 0  OutDiscards : 0  OutNoRoutes : 0
ReasmTimeout : 60  ReasmReqds : 0  ReasmOKs : 0
ReasmFails : 0  FragOKs : 0  FragFails : 0
FragCreates : 0  RoutingDiscards: 0
```

```c
rispix#config t
Enter configuration commands, one per line. End with CNTL/Z.
rispix(config)#in ch 0/1
rispix(config-if)#no offload e200 50
rispix(config-if)#end
rispix#show ext ch 0/1 ip-stack
...No IP statistics found
```

[CSCdk45042]

• The TCP connection is closed (a FIN sent) before all data is sent. The remaining data (1 to 12 bytes) is sent after the connection is closed with another FIN. This problem occurs only with TCP connections that include TCP options in the TCP header, and if the remaining data to be sent on the connection will fill up the packet before taking into account the length of the TCP options (12 bytes). This problem occurs when using the TCP large window support, which utilizes the TCP Timestamp option, implemented per RFC 1323.

The workaround is to complete the following tasks:

---

**Step 1** Log into the Cisco Mainframe Channel Connection (CMCC) console:

```
if-con <CCMCC Slot> c
```

**Step 2** Display the current state of this RFC:

```
ipconf <Offload IP Address> tcp_rfc1323
```

**Step 3** Disable this RFC:

```
ipconf <Offload IP Address> tcp_rfc1323 off
```
Step 4 Verify the configuration change using Step 2. This RFC can be re-enabled, if necessary, using the same command but with the “on” option.

ipconf <Offload IP Address> tcp.rfc1323 on

Step 5 Exit the CMCC console:

quit (CIP21-x/CIP204-x releases)
if-quit or ^C^C^C (CIP22-x/CIP205-x and all later releases or XCPA26-x/XCPA214-x and all later releases)

Unlike configuration commands issued from the router console, this CMCC configuration command is not retained if the CMCC or the router reloads or crashes and reloads. [CSCdk57139]

• When running the CMCC TN3270 server, logical unit (LU) 1 print jobs hang if the print application sends the RU chains as EXR (exception response) and the connection is running over a RFC1646-style TN3270 print connection.

The workaround is to print the job using LU 3 printing or to reconfigure the print application to send the SNA RU chains with DR (definite response) requested. [CSCdk59063]

• IP datagram connectivity no longer works if the following message appears on the router log for each IP datagram packet sent to the host:

%PKTS-3-NOSUPP:

There is no workaround. [CSCdk67396]

Open Caveats in Version 26.2/Resolved Caveats in Version 26.4

This section describes possible unexpected behavior in Version 26.2. All the caveats listed in this section are resolved in Version 26.4.

• After shutting down the Cisco Mainframe Channel Connection (CMCC) physical interface, the channel MIB variables, cipCardDtrBrdStatus, cipCardDtrBrdSignal and cipCardDtrBrdOnline, show the values prior to shutting down the interface instead of the current values. The information displayed on a show ext ch x/y subchannel command does not reflect the current state of the CMCC card.

There is no workaround. [CSCdj78246]

• When running the Cisco Mainframe Channel Connection (CMCC) Offload feature, the WRONGDESC error message was displayed if the host application issues a socket purge request using the host descriptor instead of the offload box socket descriptor. Socket purge requests are normally issued by VM/MVS/TPF TCP/IP applications when closing a socket.

The message is misleading because the host application must sometimes use the host descriptor if it has not been notified of the offload box socket descriptor. This occurs when an error is detected during socket connection establishment. The WRONGDESC error message has been removed. [CSCdj92653]

• During a brief TCP connection, the Cisco Mainframe Channel Connection (CMCC) TCP/IP Offload feature fails to return a response to a Read/Recv type socket request, causing the connection’s host application to hang while waiting for a response.

A window exists for brief TCP connections when a connection is made with TCP/IP on the CMCC and then broken (FIN received) before Offload has received and processed an Accept socket request from the host. In this situation, Offload misses the notification from TCP/IP that the connection had been terminated.

There is no workaround. [CSCdk12291]
The Cisco Mainframe Channel Connection (CMCC) TN3270 server session switch feature (DLUR End Node) does not support parallel transmission groups (TGs). Only one LLC link is permitted between the end node and each of its adjacent APPN nodes. Parallel TGs can be used to provide redundancy. [CSCdk15431]

An architectural constraint causes the Cisco Mainframe Channel Connection (CMCC) TN3270 server's DLUR to report only approximately 20 of the links to DLUS. This prevents LU-LU sessions from being routed over the unreported links. The topology database update (TDU) message reporting the links is limited to 1024 bytes. In order to report more links, DLUR has to send multiple TDUs. The workaround is that once the DLUR-DLUS pipe is established additional links will be reported if they become active. [CSCdk15446]

After changing or removing a configured virtual routing node (VRN) on a Cisco Mainframe Channel Connection (CMCC) TN3270 server dlur lsap, VTAM still shows the VRN D NET,TOPO,ORIG=dlurname,DEST=vrnname as OPER. VTAM shows the resource sequence number (RSN) as odd, indicating some uncertainty. This uncertainty is because DLUR fails to increment the RSN when sending the TDU (topology database update) generated by the VRN name change. A workaround is to close and then reopen the DLUS-DLUR pipe by using the VTAM V NET,INACT,ID=dlurname command. This does not disrupt the LU-LU sessions if the dependent PUs are configured ANS=CONT. New sessions cannot be established while the pipe is down. [CSCdk21067]

BADTIMER messages appear when running the TN3270 server. In this case, the messages appear because a TN3270 session is being negotiated or recently has been negotiated. The messages do not impact normal TN3270 server operations. There is no workaround. [CSCdk21633]

During connection, the Cisco Mainframe Channel Connection (CMCC) TN3270 server delays sending DEVTYPE IS to the client for up to one minute. The client shows a blank screen during the delay if the client requests connection to a specific logical unit (LU), and that LU only became available within the last 6 seconds. The delay is generally much shorter than one minute. It is only that long if there are clients in the network taking 30 to 40 seconds to respond to the Timing Mark. The workaround is to delay reconnecting for 6 seconds or to disconnect and reconnect immediately upon noticing the delay. [CSCdk28081]

When using a logon manager through Cisco Mainframe Channel Connection (CMCC) TN3270 DLUR, the logon manager queues a session for the SLU to recover the session after the user has finished an application. VTAM sends UNBIND 02 (bind forthcoming). The CMCC TN3270 server logical unit (LU) sends an UNBIND +RSP and the DLUR sends SESSEND with code 0A (SSCP gone). This forces SSCP to clean up the queued session from the logon manager. The expected PREALC-P session from the logon manager no longer exists. Using the CMCC TN3270 server DLUR EN capability, connect to a logon manager such as NetView access or TPX. [CSCdk29362]

This section describes possible unexpected behavior in Version 26.1. All the caveats listed in this section are resolved in Version 26.2.

- When running the Cisco Mainframe Channel Connection (CMCC) TN3270 server, the CMCC adapter reports fatal error 35 and reloads. This error occurs when the CMCC adapter is running low on memory and a packet arrives that is larger than the SNA inbound request/response unit (RU) size. Typically, this error occurs when the router is running transports such as FDDI between the CMCC adapter and the client.

  The workaround is to increase the inbound RU size defined in the host logmode tables. [CSCdj76007]

- With Offload, a socket can be closed in a way that the control block lingers for 60 seconds. If an attempt is made to re-establish the same connection before the 60 second period has expired, connection failure might occur. [CSCdj80952]

- Stronger type checking was added to allow recovery from internal errors. These errors should not occur in normal use. [CSCdj90536]

- When aborting and restarting a remote APPN mode while connectionless traffic is flowing, the following error messages are displayed:

  %CMPCTG-3-LS_PSM_ERR: TG Name: CMPCTG -CnlsLs, Event ITestInd, State SClnsConnected %MBUF-0-MFREEEx2: mfree: mbuf 845F0160 already freed from pc=8015D228 ra=80044040 @(pc=80057F20ra=80044040)

  This is a cosmetic problem. There is no workaround. [CSCdj91905]

- The MSG_PEEK flag on the RECV, RECVwait, and RECVwaitFORfin socket requests was ignored (for example, RECV requests were treated like READ requests). This error causes transaction processing facility (TPF) offload applications to drop incoming data if MSG_PEEK was used with RECV requests.

  There is no workaround. [CSCdk00532]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails because of corruption in SNA-related code. Very small timing windows, which occur in unreliable or high latency networks, can cause this failure. These networks create many asynchronous balanced mode extended (SABMEs), which can trigger this bug.

  The workaround is to tune the LLC timers to reflect true delays in the network. [CSCdk02032]

- Cisco Mainframe Channel Connection (CMCC) adapter crashes with fatal error 35. The CMCC adapter reports the following message:

  bad LU on DISC...

  This error is caused by CSCdj81522. The crash might occur if a TN3270E client connects and does not negotiate bind-image.

  The workaround is to ensure that all clients support bind-image. [CSCdk02535]

- Repeated inact/act of the external communication adapter (XCA) major node or the switched major node causes the TN3270 PUs to become stuck in a RESET/XID cycle.

  The workaround is to **shut** and then **no shut** the TN3270 server. [CSCdk03985]

- The Cisco Mainframe Channel Connection (CMCC) TN3270 server connects and then disconnects a client. This occurs with LOGAPPL applications when the client sends data to the host application and the host response to Notify reaches the server after the bind.

  The workaround is to reconnect. [CSCdk06887]
• A connection can be terminated if the flowoff condition is reached. [CSCdk07022]

• When the Cisco Mainframe Channel Connection (CMCC) receives a corrupted XID3 message, the CMCC adapter spontaneously reloads with the message:

```c
%SIS802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/mpcxid.C @ 66 - nextCv <= (Cv *) ((byte *) &fmtType + xidLength)
```

The workaround is to fix the component that is generating the corrupted XID3 message. See CSCdk10071. [CSCdk08437]

• During bulk transfer operations that move data to the host, throughput to the host is limited by overhead on the channel causing channel utilization to approach 100 percent. Use the `show controller cbus` command to determine the ECA utilization. The ECA statistic is updated once a minute.

There is no workaround. [CSCdk08438]

• The Cisco Mainframe Channel Connection (CMCC) microcode reports a fatal error and reloads. This is an infrequent problem that occurs when there is a very small timing window. [CSCdk08533]

• The client is disconnected when the host sends a DACTLU followed by an ACTLU. In VTAM through cross-domain, the host can send a DACTLU followed by an ACTLU to clean up the logical unit (LU) session, but not to disconnect the LU session. [CSCdk08642]

• The Cisco Mainframe Channel Connection (CMCC) microcode reports a fatal error and reloads. This error occurs when unconnected PUs attempt to send XIDs and TEST frames to the host. The PU timer expires and corrupts the TN3270 server timer-queue. This error occurs when the PU disconnects or when a NULL XID is about to be sent to the host.

The workaround is to ensure that all PUs are either shut down or connected. [CSCdk09978]

• When the connection to a host from the Cisco Mainframe Channel Connection (CMCC) TN3270 server is not by way of the channel, data corruption might occur, resulting in bad XIDs or binds being reported.

There is no workaround. [CSCdk10071]

• The TN3270 user cannot log on because the keyboard is locked. The keyboard can lock if a TN3270 user presses an invalid AID key (such as PF or PA) before logging on to a host application. This does not occur with TN3270 clients or LOGAPPL logical units (LUs).

The workaround is to locally clear the keyboard lock, if the client supports this feature. Otherwise, the user must disconnect and reconnect. [CSCdk10200]

• The TN3270 server refuses new TCP connections. This problem lasts for 2 to 20 minutes depending on the number of TCP requests, and occurs when one-way network congestion exists between one or more clients and the server. The congestion direction must be from the server to the client. The congestion causes the client not to see the SYN/ACK coming from the server so the client resends the SYN.

There is no workaround. [CSCdk11113]

• When using TN3270 server to connect to NetView when the NetView type ahead feature is used, the LU-LU session can be stopped with a PROG MSG.

The workaround is to recycle the logical unit (LU) in VTAM and restart the session. [CSCdk11361]

• The Cisco Mainframe Channel Connection (CMCC) adapter reports the IPC-NO-MEMD message and hangs. This occurs when CMCC adapter host communications are cut off before a hierarchical reset. [CSCdk11787]
• Cisco Mainframe Channel Connection (CMCC) TN3270 server DLUR session is unbound by DLUS with sense 1002 (RU length error) soon after the DLUR-DLUS pipe is established. This error occurs when 10 or more LLC links connected to DLUR generate a topology database update (TDU) to DLUS that exceeds the maximum RU size specified in the bind. The CP-CP session can fail with the same sense code for the same reason. In this case, the RU that exceeds the maximum RU size is the one specified in the location that DLUR sends to find the DLUS.

The workaround is to reduce the number of LLC links available to DLUR until the DLUR-DLUS pipe is established. [CSCdk11790]

• When the MSG_PEEK flag is set on a RECV, RECVwait, or RECVwaitFORfin socket request, only the Offload message header and response header are returned to the host. The buffer length field in the Offload message header indicates MSG_PEEK data is present in the message but no data is sent to the host. This problem causes TPF offload applications to collect invalid data when accessing the MSG_PEEK data.

There is no workaround. [CSCdk14244]

• An error in the channel connection causes incorrect channel events, sometimes accompanied by LOGDATA, resulting in an SSI_ASSERT in attn_state_fsm in cta/cta.c with the following message:

SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../cta/cta.c @ 350 - FALSE

There is no workaround. The user must cycle the external communication adapter (XCA) node. [CSCdk14424]

Open Caveats in Version 26.0/Resolved Caveats in Version 26.1

This section describes possible unexpected behavior in Version 26.0. All the caveat s listed in this section are resolved in Version 26.1.

• The Cisco Systems Network Architecture (CSNA) responds to single router explorers with a specific router instead of an all routers explorer response. [CSCdi64614]

• After certain low memory conditions, Cisco MultiPath Channel (CMPC) fails to recover. [CSCdi77372]

• If the channel transport adapter device registers after the LLC2, the LLC2 informs the channel transport adapter of the connection count. [CSCdj32856]

• Under certain conditions during memory allocation, the CIP can encounter a fatal error upon completion of a direct memory access transfer from or to MEMD. The fatal error code is typically 35 and it can coincide with the following message:

*RSP-3-RESTART: Interface Channel4/x, output stuck

This error can be triggered by all software features with the exception of Common Link Access to Workstation (CLAW) IP datagram. It is more likely to occur with features that use a lot of memory, like the TN3270 server. [CSCdj52480]

• The Cisco Mainframe Channel Connection (CMCC) adapter reports a BSQ-x-SRB_CHAIN error message indicating that the read SCB chain is out of sequence. The problem is caused by unusual conditions during status presentation such as ESCON link errors.

There is no workaround. [CSCdj61319]

• The Cisco Mainframe Channel Connection (CMCC) TCP/IP stack uses path MTU discovery (RFC 1191) to select the size of an outgoing IP packet. The algorithm used does not work if the IP layer adds IP options to the packet. If this situation occurs, TCP connections will hang and eventually time out as soon as they try to send a segment larger than the smallest MTU in the path. Of all the problems that could lead to dropped TCP connections because of path MTU discovery, this is
probably the least likely to occur. It is much more common that the problem is caused by an
improperly designed network (for instance, a configuration with a bridge connecting two networks
with different MTUs) or a misconfigured router that does not send an ICMP type “Destination
unreachable” with code “Fragmentation needed but DF bit set”.

To confirm that the IP option caused path MTU discovery not to work, get a sniffer trace to show
the TCP segments from the CMCC adapter as well as any ICMPs going back to it. If the router that
sends the ICMPs is the CMCC router, collect the output of the following commands before and after
a session is dropped:

- `show extended channel slot/port ip-stack`
- `show extended channel slot/port icmp-stack`
- `show extended channel slot/port tcp-stack`
- `show ip traffic`

[CSCdj65774]

- In networks with a high volume of type 1 traffic (typically XIDs) the VTAM might combine many
type 1 messages in a block, mistakenly causing the frame to appear badly formed and resulting in
the ASSERT message and an automatic reload of the Cisco Mainframe Channel Connection
(CMCC) image. This problem occurs only with cip21-19 images and earlier. It does not happen with
cip22-xx and higher.

The workaround is to artificially limit the rate at which remote stations can connect by adding delays
to a startup script. [CSCdj69281]

- The kernel timeout function hits a fatal error when called with a negative time value. For example,
this will happen if the Offload code gets a connect request with a timeout value of 0x7fffffff seconds.
The workaround for the offload problem is to reconfigure for IP datagram mode. There is no
workaround available for the bug in the kernel timeout function. [CSCdj72646]

- On a Cisco 7000 series router with a CIP, if all interfaces on the CIP are shut down when the CIP is
loaded, then the interprocess communication (IPC) subfacility will not work on the CIP even after
`no shut` commands are issued for the interfaces. [CSCdj74844]

- The Cisco Mainframe Channel Connection (CMCC) TN3270 sessions can linger for up to 10
minutes after the PU that the sessions ran through is shut down. This situation causes subsequent
activations of the external communication adapter (XCA) major node to fail at the host because the
CMCC adapter/SAP is not ready to open.

A workaround is to issue a `shut` and then a `no shut` command on the TN3270 server, causing the
connections to be brought down quickly. [CSCdj76280]

- Following a `reload`, `microcode reload`, or after a `no shutdown` command is issued, IBM MVS
TCP/IP could complain about channel status of x'06'. This problem occurs following a resetting event
condition where MVS IOS expected to have cleared the resetting event condition prior to the event
actually occurring. The recovery mechanism that is already in place should recover from this error.
If the channel interface is always shut down prior to a reload or microcode reload and this fix is
applied, the host should stop complaining about the channel status of x'06'. [CSCdj78947]

- The Cisco Mainframe Channel Connection (CMCC) adapter reloads spontaneously after the
following error message:

%CTA-0-UNEXP_LSI_CMD: PA1 CTA C020-56 received LSI command 0x4D11 at 0x8042CA8C
An unrecognized command code was recognized during communication between the LLC2 and Cisco Systems Network Architecture (CSNA) components on the CMCC adapter. This problem has never been detected in customer use, and has only been seen during the debugging of a new feature. However, the problem could be caused by configuring High Performance Routing (HPR) in a remote device.

The workaround is to reconfigure the remote device to not specify HPR. [CSCdj79403]

- The Cisco Mainframe Channel Connection (CMCC) adapter reports fatal error 35 when running TN3270. Before the fatal error, the CMCC adapter reports the following error message:

```
%CIP24-4-MSG: %TN3270S-4-NO_LU_SESSIONS: No LU sessions left for PUs at IP addr a.b.c.d, port x
```

The problem might occur when the maximum-lu limit has been reached or when no more logical units (LUs) are available at a given TN3270 server listening point.

The workaround is to increase the maximum-lu limit to a level that will not be reached during operation of the server. Also, the user should increase the number of PUs (really, logical units [LUs]) on each listening point. [CSCdj80602]

- This problem results in the mainframe complaining about SIOCC2, which is a start I/O condition code 2. SIOCC2 is an indication that the device is busy for an extended period of time. Without this fix, the problem can be worked around by shutting down the Cisco Mainframe Channel Connection (CMCC) interface and then bringing it up again. [CSCdj80886]

- The Cisco Systems Network Architecture (CSNA) responds to the TEST command when no SAP is active. This error might result in an end station trying to connect to a Cisco Mainframe Channel Connection (CMCC) adapter that has no connectivity to the host. This situation occurs when the CSNA interface is shut down manually or by other media problems (for example, a loose cable). [CSCdj80925]

- With Offload, a socket can be closed in a way that the control block lingers for 60 seconds. If an attempt is made to re-establish the same connection before the 60 second period has expired, connection failure might occur. [CSCdj80952]

- The Cisco Mainframe Channel Connection (CMCC) Offload code prints an OFFL-0-WRONGFREE error message and hits a fatal error. This problem occurs if the read channel program ends in the middle of a socket response that spans more than one Common Link Access to Workstation (CLAW) buffer and a halt subchannel is issued before the read channel program resumes.

There is no workaround. [CSCdj80990]

- During the recovery from certain error conditions in the Cisco Mainframe Channel Connection (CMCC) TN3270 server, the CMCC adapter might sometimes report a fatal error 35 and spontaneously reload. [CSCdj81522]

- The Cisco Mainframe Channel Connection (CMCC) microcode might log the message “fatal error 35” and spontaneously reload. This situation can happen if the CMCC TN3270 server session switch (DLUR) feature is being used and either the DLUR component or TN3270 server is shut down or deconfigured while there are configured DLUR links. The workaround is to remove the DLUR links first, using no link name. [CSCdj82232]

- The Cisco Systems Network Architecture (CSNA) fails to send disconnect when indication buffer is in use. This causes the following results: the end-station cannot connect back in, and if the connection is flow-off, it will remain in flow-off state. [CSCdj82785]

- With certain TN3270 client software, the user can successfully establish an LU-to-LU session, but when the user enters the first data after the bind, the Cisco Mainframe Channel Connection (CMCC) TN3270 server disconnects the client. The CMCC TN3270 server logs the fact that it received invalid Telnet data from the client.
The problem occurs only with certain clients (for example, PC3270 and Attachmate) and when the user enters data before the host application sends out its first screen (most applications send a screen of data immediately after the bind, start data traffic).

Because the problem only occurs in TN3270E mode, and some clients have an option to disable TN3270E mode, it is possible to bypass this problem in situations where TN3270E mode is not required. The alternatives are to use a different client or change the host application. [CSCdj84064]

- When a TN3270E client connects to a Cisco Mainframe Channel Connection (CMCC) TN3270 server and enters a logon request, the server sometimes discards the request and sends a “-B” message to the client. This message becomes appended on the screen, to the logon request data. If the user now presses enter, the host replies with the following message:

  "unsupported function".

This problem occurs if the same logical unit (LU) can be used by TN3270 and TN3270E clients. The workaround is to retry the logon request. [CSCdj84122]

- In some customer environments, LOGDATA records that consist of multiple error messages can result from the mainframe not responding to device level activity for longer than 500 ms. The ESCON architecture states that this timeout value can range from 400 ms to 850 ms. To avoid some of the occurrences of LOGDATA, adjust the timeout from 500 ms to 800 ms. [CSCdj84218]

- Additional information was added to the Cisco Mainframe Channel Connection (CMCC) fatal error output report. This data helps identify the events leading up to the failure. [CSCdj85568]

- The channel transport architecture device is informed of the connection count irrespective of the order in which the channel transport adapter and LLC2 register. [CSCdj87846]

- The Cisco Mainframe Channel Connection (CMCC) DLUR repeatedly tries to establish CP-CP sessions with an incompatible NN server and fails to try other NN server links under the following conditions:
  - The CMCC TN3270 server DLUR/DLUS with the preferred NN server is configured; the DLUR is varied inactive by lu/cpname and is defined statically on the primary host as cross-domain resource (CDRSC) or logical unit (LU), then the link between the primary and the CMCC adapter is left active. This situation makes a controlled SSCP takeover difficult.

  The workaround is to not configure preferred-NN server. [CSCdj87854]

- When running fast mainframe processors in offload mode, 10-20 percent of the channel bandwidth can be wasted by improperly handling the more-to-come processing within the Common Link Access to Workstation (CLAW) protocol.

  There is no workaround. [CSCdj88636]

- If a DMA write error occurs on the CIP in the process of sending a packet to the Cisco IOS software, the CIP could go into an infinite loop when the CIP interface the DMA error occurred on is shut down or the router performs a cbus complex restart. [CSCdj90280]

- At `show ext cn/2 pu/lu`, some DDDLU LU names appear blank if host applications send NULL SLU data in the bind.

  There is no workaround. [CSCdj90734]

- Sometimes outbound data is randomly corrupted. This situation occurs with Cisco Mainframe Channel Connection (CMCC) images in Cisco IOS Release 11.2(BC) if the TN3270 PUs are attached to VTAM by Token Ring (rather than channel attached) and some clients are running 3270 extended datastream. The problem usually occurs after file transfer of binary data.

  There is no workaround. [CSCdj90738]
Caveats for CIP and CPA Microcode

- A reset of the CIP virtual interface configured with LLC2 can cause MEMD buffer errors resulting in a cbus complex restart. [CSCdj90822]

- The Cisco Mainframe Channel Connection (CMCC) TN3270 server command `show extended ch x/2 tn3270 pu lu history` might cause the router to reload. This situation happens if the logical unit (LU) history buffer contains an event indicating that it received data from the client after it sent unbind to the client. The workaround is to not use the `show lu history` command. [CSCdj91756]

- When the maximum-lu is reached, clients cannot connect for a few minutes. Usually only one listening point is affected. The workaround is to increase the maximum-lu in the configuration so that the maximum-lu will not be reached. [CSCdj92158]

- The Cisco Mainframe Channel Connection (CMCC) adapter returned User Datagram Protocol (UDP) data with 32 bytes less than expected to the host application under transaction processing facility (TPF). TCP/IP running Offload is not affected by this problem. There is no workaround. [CSCdj93915]

- An attempt to activate an SNA local node where Cisco Mainframe Channel Connection (CMCC) statements define the subchannels but for which no corresponding transmission group (TG) statement exists, resulting in an unexpected reload. The workaround is to make sure the TG statement is configured before the associated CMCC statements. [CSCdk01922]

- The Cisco Mainframe Channel Connection (CMCC) adapter fails because of corruption in SNA-related code. Very small timing windows, which occur in unreliable or high latency networks, can cause this failure. These networks create many Set Asynchronous Balanced Mode Extended (SABMEs), which can trigger this bug. The workaround is to tune the LLC timers to reflect true delays in the network. [CSCdk02032]

- Cisco Mainframe Channel Connection (CMCC) adapter crashes with fatal error 35. The CMCC adapter reports the following message:

  bad LU on DISC...

  This error is caused by CSCdj81522. The crash might occur if a TN3270E client connects and does not negotiate bind-image. The workaround is to ensure that all clients support bind-image. [CSCdk02535]

- An attempt to configure more than 32 transmission groups (TG) using the Cisco Mainframe Channel Connection (CMCC) might cause the CMCC to reload. The workaround is to limit the number of TG statements to 32. The changes incorporated by this DDTS increase the TG limit to 64. [CSCdk03733]

- When the Cisco Mainframe Channel Connection (CMCC) receives a corrupted XID3 message, the CMCC adapter spontaneously reloads with the message:

  %SSI802-3-FATAL_ERROR: SSI_ASSERT failure in ../mpc/mpcxid.C @ 66 - nextCv <= (Cv *) (((byte *) &fmtType + xidLength)

  The workaround is to fix the component that is generating the corrupted XID3 message. See CSCdk10071. [CSCdk08437]
• When the connection to a host from the Cisco Mainframe Channel Connection (CMCC) TN3270 server is not by way of the channel, data corruption might occur, resulting in bad XIDs or Binds being reported.
  There is no workaround. [CSCdk10071]

**Related Documentation**

All of the documentation in this section is available online and on the Documentation CD-ROM. Some publications are available as printed documents.

**Hardware Documentation**

This section provides information about available hardware-specific documentation including CIP, CPA, and platform-specific hardware publications.

**Cisco 7000 Series Hardware Documentation**

For hardware installation and configuration information on the CIP or CIP2, refer to the following publications:

- *Channel Interface Processor (CIP) Installation and Configuration* (DOC-781342=)
- *Second-Generation Channel Interface Processor (CIP2) Installation and Configuration* (DOC-783335=)
- *Upgrading DRAM on the CIP2* (DOC-783915=)

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-7010IM2=)

**Cisco 7200 Series Hardware Documentation**

For hardware installation and configuration information on the CPA, refer to the following publications:

- *PA-1C-E ESCON Channel Port Adapter Installation and Configuration*
- *PA-4C-E 1-Port High Performance ESCON Channel Port Adapter Installation and Configuration*
- *PA-1C-P Parallel Channel Port Adapter Installation and Configuration*

For a complete list of chassis-specific hardware documentation for the Cisco 7200 series routers refer to the following master index:

*Cisco 7200 Series Routers Documentation Master Index*
Cisco 7500 Series Hardware Documentation

For hardware installation and configuration information on the CIP or CIP2, refer to the following publications:

- **Channel Interface Processor (CIP) Installation and Configuration** (DOC-781342=)
- **Second-Generation Channel Interface Processor (CIP2) Installation and Configuration** (DOC-783335=)
- **Upgrading DRAM on the CIP2** (DOC-783915=)

For a complete list of chassis-specific hardware documentation for the Cisco 7500 series routers refer to the following master index:

*Cisco 7500 Series Routers Documentation Master Index*

Release-Specific Documentation

The documentation in this section includes Cisco IOS software release publications, which can be found on Cisco.com.

For documentation of CIP and CPA features in Cisco IOS Release 12.2 T, refer to the publications in Table 7.

**Table 7  Cisco IOS Release 12.2T Publications**

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.2T Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 12.2 T</td>
<td>OL-2339-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 T</td>
<td>78-12946-xx</td>
</tr>
<tr>
<td>12.2 T New Features and System Error Messages</td>
<td>n/a</td>
</tr>
</tbody>
</table>

For documentation of CIP and CPA features in Cisco IOS Release 12.2, refer to the publications in Table 8.

**Table 8  Cisco IOS Release 12.2 Publications**

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.2 Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 12.2</td>
<td>OL-1614-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 BW</td>
<td>OL-3166-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 BY</td>
<td>OL-3271-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 DD</td>
<td>OL-1226-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 DX</td>
<td>OL-2930-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 MB</td>
<td>78-13338-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 XA</td>
<td>OL-1670-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 XB</td>
<td>OL-1837-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 YD</td>
<td>OL-2709-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 YE</td>
<td>OL-2613-xx</td>
</tr>
</tbody>
</table>
Table 8  Cisco IOS Release 12.2 Publications (continued)

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.2 Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 YJ</td>
<td>OL-2850-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 YX</td>
<td>OL-3617-xx</td>
</tr>
<tr>
<td>New Features in Cisco IOS Release 12.2</td>
<td>n/a</td>
</tr>
</tbody>
</table>

For documentation of CIP and CPA features in Cisco IOS Release 12.1 T, refer to the publications in Table 9.

Table 9  Cisco IOS Release 12.1 T Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.1 T Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 12.1</td>
<td>OL-2893-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.1 T</td>
<td>78-10811-xx</td>
</tr>
<tr>
<td>Cisco IOS Release 12.1 T New Features</td>
<td>n/a</td>
</tr>
</tbody>
</table>

For documentation of CIP and CPA features in Cisco IOS Release 12.1, refer to the publications in Table 10.

Table 10  Cisco IOS Release 12.1 Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.1 Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Configuration Fundamentals Configuration Guide</td>
<td>DOC-7810222=</td>
</tr>
<tr>
<td>Cisco IOS Configuration Fundamentals Command Reference</td>
<td>DOC-7810223=</td>
</tr>
<tr>
<td>Cisco IOS Bridging and IBM Networking Configuration Guide</td>
<td>DOC-7810256=</td>
</tr>
<tr>
<td>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</td>
<td>DOC-7810257=</td>
</tr>
<tr>
<td>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</td>
<td>DOC-7810520=</td>
</tr>
<tr>
<td>Cisco IOS Command Summary, Volume 1 of 2</td>
<td>DOC-7810262=</td>
</tr>
<tr>
<td>Cisco IOS Command Summary, Volume 2 of 2</td>
<td>DOC-7810262=</td>
</tr>
<tr>
<td>Cisco IOS System Error Messages</td>
<td>DOC-7810263=</td>
</tr>
<tr>
<td>Cisco IOS Debug Command Reference</td>
<td>DOC-7810264=</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 12.1</td>
<td>OL-2893-xx</td>
</tr>
</tbody>
</table>

For documentation of CIP and CPA features in Cisco IOS Release 12.0 T, refer to the publications in Table 11.

Table 11  Cisco IOS Release 12.0 T Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.0 T Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 12.0</td>
<td>OL-2881-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0 T</td>
<td>78-6055-xx</td>
</tr>
<tr>
<td>Cisco IOS Release 12.0 T New Features</td>
<td>n/a</td>
</tr>
</tbody>
</table>
For documentation of CIP and CPA features in Cisco IOS Release 12.0, refer to the publications in Table 12.

Table 12  Cisco IOS Release 12.0 Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 12.0 Publication</th>
<th>Customer Order Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Fundamentals Configuration Guide</td>
<td>DOC-785829=</td>
</tr>
<tr>
<td>Configuration Fundamentals Command Reference</td>
<td>DOC-785830=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Configuration Guide</td>
<td>DOC-785850=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Command Reference</td>
<td>DOC-785851=</td>
</tr>
<tr>
<td>Cisco IOS Software Command Summary</td>
<td>DOC-785859=</td>
</tr>
<tr>
<td>Cisco IOS Software System Error Messages</td>
<td>DOC-785860=</td>
</tr>
<tr>
<td>Debug Command Reference</td>
<td>DOC-785858=</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 12.0</td>
<td>OL-2881-xx</td>
</tr>
</tbody>
</table>

For documentation of CIP and CPA features in Cisco IOS Release 11.3 T, refer to the publications in Table 13.

Table 13  Cisco IOS Release 11.3 T Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 11.3 T Publication</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 11.3</td>
<td>78-4998-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco 7000 Family for Cisco IOS Release 11.3 T</td>
<td>78-5015-xx</td>
</tr>
<tr>
<td>Cisco IOS Release 11.3 T New Features</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Only the CIP is available in Cisco IOS Release 11.3 and below.

For documentation of CIP features in Cisco IOS Release 11.3, refer to the publications in Table 14.

Table 14  Cisco IOS Release 11.3 Publications

<table>
<thead>
<tr>
<th>Cisco IOS 11.3 Release Publication</th>
<th>Customer Order Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Fundamentals Configuration Guide</td>
<td>DOC-CFCG11.3=</td>
</tr>
<tr>
<td>Configuration Fundamentals Command Reference</td>
<td>DOC-CFCR11.3=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Configuration Guide</td>
<td>DOC-IBMNCG11.3=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Command Reference</td>
<td>DOC-IBMNCR11.3=</td>
</tr>
<tr>
<td>Cisco IOS Software Command Summary</td>
<td>DOC-CIOSCS11.3=</td>
</tr>
<tr>
<td>System Error Messages</td>
<td>DOC-SYSEM11.3=</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 11.3</td>
<td>78-4998-xx</td>
</tr>
</tbody>
</table>

For documentation of CIP features in Cisco IOS Release 11.2 BC, refer to the publications in Table 15.
Table 15 Cisco IOS Release 11.2 BC Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 11.2 BC Publication</th>
<th>Customer Order Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Cisco IOS Release 11.2</td>
<td>78-3648-xx</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 11.2 BC</td>
<td>78-4694-xx</td>
</tr>
<tr>
<td>Feature Guide for Cisco IOS Release 11.2 BC</td>
<td>78-4693-xx</td>
</tr>
</tbody>
</table>

For documentation of CIP features in Cisco IOS Release 11.2, refer to the publications in Table 16.

Table 16 Cisco IOS Release 11.2 Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 11.2 Publication</th>
<th>Customer Order Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Fundamentals Configuration Guide</td>
<td>DOC-CFCG11.2=</td>
</tr>
<tr>
<td>Configuration Fundamentals Command Reference</td>
<td>DOC-CFCR11.2=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Configuration Guide</td>
<td>DOC-IBMNCG11.2=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Command Reference</td>
<td>DOC-IBMNCR11.2=</td>
</tr>
<tr>
<td>Cisco IOS Software Command Summary</td>
<td>DOC-CIOSCS11.2=</td>
</tr>
<tr>
<td>System Error Messages</td>
<td>DOC-SYSEM11.2=</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 11.2</td>
<td>78-3648-xx</td>
</tr>
</tbody>
</table>

For documentation of CIP features in Cisco IOS Release 11.1, refer to the publications in Table 17.

Table 17 Cisco IOS Release 11.1 Publications

<table>
<thead>
<tr>
<th>Cisco IOS Release 11.1 Publication</th>
<th>Customer Order Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Fundamentals Configuration Guide</td>
<td>DOC-CFCG11.1=</td>
</tr>
<tr>
<td>Configuration Fundamentals Command Reference</td>
<td>DOC-CFCR11.1=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Configuration Guide</td>
<td>DOC-IBMNCG11.1=</td>
</tr>
<tr>
<td>Bridging and IBM Networking Command Reference</td>
<td>DOC-IBMNCR11.1=</td>
</tr>
<tr>
<td>Cisco IOS Software Command Summary</td>
<td>DOC-CIOSCS11.1=</td>
</tr>
<tr>
<td>System Error Messages</td>
<td>DOC-SYSEM11.1=</td>
</tr>
<tr>
<td>Release Notes for Cisco IOS Release 11.1</td>
<td>78-2886-xx</td>
</tr>
</tbody>
</table>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.
Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport
You can access the Cisco website at this URL:
http://www.cisco.com
You can access international Cisco websites at this URL:

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:
http://www.cisco.com/univercd/home/home.htm
The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:
http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:
http://www.cisco.com/go/marketplace/docstore
If you do not have a user ID or password, you can register at this URL:

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
From this site, you will find information about how to do the following:
• 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:


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 have identified a vulnerability in a Cisco product, contact PSIRT:

• For emergencies only — security-alert@cisco.com
  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
• For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:
• 1 877 228-7302
• 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

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


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

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.
To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:


To register as a Cisco.com user, go to this URL:


## Obtaining Technical Assistance

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

### Cisco Support Website

The Cisco 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 at this URL:


Access to all tools on the Cisco 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:


---

**Note**

Before you submit a request for service online or by phone, use the Cisco Product Identification Tool to locate your product serial number. You can access this tool from the Cisco Support website by clicking the Get Tools & Resources link, clicking the All Tools (A-Z) tab, and then choosing Cisco Product Identification Tool from the alphabetical list. This 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.

---

**Tip**

**Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the Advanced Search link next to the Search box on the resulting page and then click the Technical Support & Documentation radio button.

To provide feedback about the Cisco.com website or a particular technical document, click Contacts & Feedback at the top of any Cisco.com web page.
Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe
• The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
  http://www.cisco.com/go/guide

• Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
  http://www.cisco.com/go/marketplace/

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

• *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
  http://www.cisco.com/ipj

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

• Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
  http://www.cisco.com/discuss/networking

• “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

• World-class networking training is available from Cisco. You can view current offerings at this URL:
This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Printed in the USA on recycled paper containing 10% postconsumer waste.