Text Part Number: 78-5266-17

Channel Port Adapter Microcode Release Note and Microcode Upgrade Requirements

July 24, 2000

This document contains the release notes for the Channel Port Adapter (CPA) microcode software. 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.

Note In this document, references to CPA correspond to both the ECPA and PCPA.

The CPA microcode is unbundled from the Cisco IOS software. Therefore, you can obtain the CPA microcode as a separately loadable software module and match a version of the CPA microcode to the Cisco IOS software. Refer to the section "CPA Microcode/Cisco IOS Software Compatibility Matrix" for more information.

Cisco IOS Release 11.3(3)T and later supports the ECPA. Cisco IOS Release 11.3(7)T and later and Release 12.0(1) and later support the PCPA. There is a default setting in the Cisco IOS software that corresponds to a particular microcode that is already loaded on the router Flash memory card or on the SanDisk memory device when a CPA is purchased as a system. Refer to the section "CPA Microcode/Cisco IOS Software Compatibility Matrix" for more information. However, when the CPA is ordered as a spare (shipped separately from a system), you might be required to download the microcode image from Cisco Connection Online (CCO).

Note We recommend that you load and use the version of CPA microcode that corresponds with your Cisco IOS software, in which case the following step is not necessary.

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

If you choose to use a version of the CPA microcode other than the one that corresponds with your Cisco IOS software, you must copy a CPA microcode image onto the router Flash memory card or SanDisk memory device and use the **microcode** router configuration command to specify this microcode image rather than the default microcode image.

For general information on CPA microcode, refer to the *PA-1C-E ESCON Channel Port Adapter Installation and Configuration* document or the *PA-1C-P Parallel Channel Port Adapter Installation and Configuration* document that shipped with the port adapter.

Introduction

This release note describes the CPA microcode caveats for the latest version of CPA microcode. It includes the CPA microcode releases described in the "CPA Microcode Release xcpa26 Caveats" section. Also included is an overview of the procedures required to upgrade to the latest versions of CPA microcode.

This CPA microcode release note discusses the following topics:

Cisco IOS Software and Cisco 7200 Family Hardware Documentation

For documentation of CPA features in the Cisco IOS Release 11.3, refer to Table 1.

Table 1 Cisco IOS Release 11.3 Publications

Cisco IOS 11.3 Release Publication	Tracking Number
Configuration Fundamentals Configuration Guide	DOC-CFCG11.3=
Configuration Fundamentals Command Reference	DOC-CFCR11.3=
Bridging and IBM Networking Configuration Guide	DOC-IBMNCG11.3=
Bridging and IBM Networking Command Reference	DOC-IBMNCR11.3=
Cisco IOS Software Command Summary	DOC-CIOSCS11.3=
System Error Messages	DOC-SYSEM11.3=
Release Notes for Cisco IOS Release 11.3	78-4998-xx

For documentation of CPA features in the Cisco IOS Release 11.3T, refer to Table 2.

Table 2 Cisco IOS Release 11.3T Publications

Cisco IOS Release 11.3T Publication	Tracking Number
Release Notes for Cisco IOS Release 11.3	78-4998-xx
Release Notes for Cisco 7000 Family for Cisco IOS Release 11.3T	78-5015-xx
Cisco IOS Release 11.3T New Features	Available on CCO only

For documentation of CPA features in the Cisco IOS Release 12.0, refer to Table 3.

Table 3 Cisco IOS Release 12.0 Publications

Cisco IOS Release 12.0 Publication	Tracking Number
Configuration Fundamentals Configuration Guide	DOC-785829=
Configuration Fundamentals Command Reference	DOC-785830=
Bridging and IBM Networking Configuration Guide	DOC-785850=
Bridging and IBM Networking Command Reference	DOC-785851=
Cisco IOS Software Command Summary	DOC-785859=
Cisco IOS Software System Error Messages	DOC-785860=
Debug Command Reference	DOC-785858=
Release Notes for Cisco IOS Release 12.0	78-6035-xx

For documentation of CPA features in the Cisco IOS Release 12.0T, refer to Table 4.

Table 4 Cisco IOS Release 12.0T Publications

Cisco IOS Release 12.0T Publication	Tracking Number
Release Notes for Cisco IOS Release 12.0	78-6035-xx
Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0T	78-6055-xx
Cisco IOS Release 12.0T New Features	Available on CCO only

For documentation of CPA features in the Cisco IOS Release 12.1, refer to Table 5.

Table 5 Cisco IOS Release 12.1 Publication

Cisco IOS Release 12.1 Publication	Tracking Number
Cisco IOS Configuration Fundamentals Configuration Guide	DOC-7810222=
Cisco IOS Configuration Fundamentals Command Reference	DOC-7810223=

Table 5 Cisco IOS Release 12.1 Publication (continued)

Cisco IOS Release 12.1 Publication	Tracking Number
Cisco IOS Bridging and IBM Networking Configuration Guide	DOC-7810256=
Cisco IOS Bridging and IBM Networking Command Reference, Volume I	DOC-7810257=
Cisco IOS Bridging and IBM Networking Command Reference, Volume II	DOC-7810520=
Cisco IOS Command Summary	DOC-7810262=
Cisco IOS System Error Messages	DOC-7810263=
Cisco IOS Debug Command Reference	DOC-7810264=
Release Notes for Cisco IOS Release 12.1	78-10724-xx

For documentation of CPA features in the Cisco IOS Release 12.1T, refer to Table 6.

Table 6 Cisco IOS Release 12.1T Publications

Cisco IOS Release 12.1T Publication	Tracking Number
Release Notes for Cisco IOS Release 12.1	78-10724-xx
Release Notes for Cisco 7000 Family for Cisco IOS Release 12.1T	78-10811-xx
Cisco IOS Release 12.1T New Features	Available on CCO only

For hardware installation and configuration information on the CPA, refer to the *PA-1C-E ESCON Channel Port Adapter Installation and Configuration* document and the *PA-1C-P Parallel Channel Port Adapter Installation and Configuration* document that shipped with the port adapter.

To obtain general information about documentation, refer to the section "Cisco Connection Online" or call customer service at 800 553-6387 or 408 526-7208. Customer service hours are 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday (excluding Cisco-observed holidays). You can also send e-mail to cs-rep@cisco.com, or you can refer to the *Cisco Information Packet* that shipped with your router.

How Does CPA Microcode Ship?

In Cisco IOS Release 11.3(3)T and later, the CPA microcode is available from the following sources:

- Electronic download from CCO using File Transfer Protocol (FTP) for all Cisco 7200-series routers
- Pre-installed on a Flash memory card or SanDisk memory device with Cisco IOS software

CPA Microcode Release xcpa27 Caveats

The following section describes the caveats to current CPA microcode versions and the modifications made in current CPA microcode versions for xcpa27 microcode. The caveats listed apply to only the most serious problems. See Table 7 for the Cisco IOS software releases supported by xcpa27 microcode.

Caveats for Version 27.8/Version 27.9 Modifications

This section describes possible unexpected behavior by Version 27.8. All the caveats listed in this section are resolved in Version 27.9. See Table 7 for the Cisco IOS software release that corresponds to the 27.9 microcode version.

- The TN3270 server disconnects the session. This occurs when a client connects to a dynamic 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 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]

- 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 server 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 message number 9.

```
CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_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 LUs can not 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 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 LU name, such as BTEST001.

  There is no workaround. [CSCdr38323]

- The TN3270 server uses an incorrect default value of 30 minutes for the max response time for the keepalive timer. This problem occurs if 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]

Caveats for Version 27.7/Version 27.8 Modifications

This section describes possible unexpected behavior by Version 27.7. All the caveats listed in this section are resolved in Version 27.8. See Table 7 for the Cisco IOS software release that corresponds to the 27.8 microcode version.

- The TN3270 server loses pool-based 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's 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 error message number 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 CMCC adapter fails with fatal error message number 35. This problem occurs when the **no client ip** *ipaddr* [*ipmask*] **pool** *poolname* command is configured when using 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 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 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 message number 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 may fail when the **shutdown** command is configured in TN3270 sub-mode.

  There is no workaround. [CSCdp99538]

- The CMCC adapter configured for CSNA may 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 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 LUs which are nailed to another subnet.

  There is no workaround. [CSCdr12567]

- The 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 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.x: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.xx:1665   N   ACT/SESS 3278S5E  9992    6147    0:0:6
  5   ABCD2005 xxx.xxx.xxx.x:1046    N   ACT/SESS 3278S5E  12731   8074    10:33:7
  6   ABCD2006 xxx.xxx.xxx.x:4033    N   ACT/SESS 3278S2E  31367   18838   2:0:51
  7   ABCD2007 xxx.xxx.xxx.x:1045    N   ACT/SESS 3278S5E  8184    4413    2:55:4
  8   ABCD2008 xxx.xxx.xxx.xx:1323   N   ACT/SESS 3278S2E  16274   7580    4:28:19
  10  ABCD200A xxx.xxx.xxx.xxx:1205  N   ACT/SESS 3278S2E  7752    4175    1:3:39
  ```

  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 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 locaddrs) 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 CMCC adapter fails with the following fatal error message number 35:

  ```
  %CTA-0-INACTIVE: PA1 CTA 7C00-50 reset after being inactive for 180 seconds
  ```

  The workaround is to shutdown the CSNA subchannel before shutting down VTAM. [CSCdr13804]

- The 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 CMCC adapter fails with fatal error message number 35. This problem occurs when the **no listen-point** TN3270 server command is configured.

  There is no workaround. [CSCdr19257]

- The CMCC adapter fails with fatal error message number 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]

Caveats for Version 27.6/Version 27.7 Modifications

This section describes possible unexpected behavior by Version 27.6. All the caveats listed in this section are resolved in Version 27.7. See Table 7 for the Cisco IOS software release that corresponds to the 27.7 microcode version.

- 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]

- 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]

- A Cisco Multipath Channel (CMPC) transmission group (TG) does not activate and the following duplicate group token message occurs:

  ```
  Get CMPCP_DUPL_TOKEN:
  ```

  This problem occurs when bringing up a TG from the host 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 CMCC adapter fails with fatal error message number 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 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 fatal error message number 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 can not 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 message number 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 CMCC adapter error occurs when host-defined 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 do not overlap with the host-defined names. [CSCdr06007]

- The TN3270 Server 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 in 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 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]

Caveats for Version 27.5/Version 27.6 Modifications

This section describes possible unexpected behavior by Version 27.5. All the caveats listed in this section are resolved in Version 27.6. See Table 7 for the Cisco IOS software release that corresponds to the 27.6 microcode version.

- BADTIMER messages appear when running 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 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 3. 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 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:

  ```
  %CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_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 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 CMCC Adapter deletes all the PUs associated with IP pool and fails with 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]

- The 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]

- 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 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]

- When the TN3270 Server statistics are displayed, a negative LU IN USE message appears. This is a cosmetic problem. LUs are still available to the clients as needed.

  There is no workaround. [CSCdp69064]

- The TN3270 Server 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 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]

Caveats for Version 27.4/Version 27.5 Modifications

This section describes possible unexpected behavior by Version 27.4. All the caveats listed in this section are resolved in Version 27.5. See Table 7 for the Cisco IOS software release that corresponds to the 27.5 microcode version.

- BADTIMER messages appear when running 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. TheTN3270 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 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 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 cip210-140, 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 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 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 CMPC and CSNA, also.

  The workaround is to upgrade the 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 CMCC Adapter TN3270 server session. If the condition continues for another 2 minutes, the 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
  ```

  [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 may 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 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 versions cip24-10 through cip24-13 and later.

  There is no workaround. [CSCdp06760]

- 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 TN3270 Server or TN3270E client fails when it connects to the server, but does not specify the name of an 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 CMCC adapter with TN3270 Server configured fails with fatal error message 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 an -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 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 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 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 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 CMCC Adapter configured for TCP/IP Offload fails with a 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 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 LU name. This problem effects all DLUR configurations and direct-connect configurations when INCLUD0E is specified in the Switched Major Node definitions.

  There is no workaround. [CSCdp34029]

Caveats for Version 27.3/Version 27.4 Modifications

This section describes possible unexpected behavior by Version 27.3. All the caveats listed in this section are resolved in Version 27.4. See Table 7 for the Cisco IOS software release that corresponds to the 27.4 microcode version.

- 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 CMCC TN3270 Server does not use this client IP address for matching on LU nailing statements in the configuration. [CSCdj44584]

- MSG10 data from one 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 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 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. TheTN3270 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 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 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 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]

- A user receives another user's 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 CMCC adapter fails with fatal error code 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 message code 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 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 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 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 non-structured 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 CMPC feature.

  There is no workaround. [CSCdp00921]

- The 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 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 CMCC fails with error message 35. The problem occurs when the TN3270 Server is using the 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]

Caveats for Version 27.2/Version 27.3 Modifications

This section describes possible unexpected behavior by Version 27.1. All the caveats listed in this section are resolved in Version 27.2. See Table 7 for the Cisco IOS software release that corresponds to the 27.2 microcode version.

- The CPA running the TN3270 Server fails with error code 35. This problem occurs when PUs are added to the configuration after the **no tn3270** command was entered.

  The workaround is to not enter the **no tn3270** command.

- 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 CMCC Adapter to reload with fatal error message 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(xxxxxxxx) or index(92)

  Where "xxxxxxxx" 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]

- The CMCC Adapter running TN3270 fails with fatal error number 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]

- 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. TheTN3270 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 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 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 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 CMCC 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 number 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 **tn-parameter code** *codevalue* command with a code value of 2.

  There is no workaround. [CSCdm54076]

- Every other CMCC 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 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 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 auto-reconnect 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 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** *minutes* 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 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() may 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 re-open the server socket by restarting the server application on the host. [CSCdm63283]

- The CMCC TN3270 server fails with fatal error code 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 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]

- 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 versions cip27-3, xcpa27-3 and later, you must configure the TN3270 **tn-parameter code** *codevalue* command with a code value of 6. [CSCdm76554]

Caveats for Version 27.1/Version 27.2 Modifications

This section describes possible unexpected behavior by Version 27.1. All the caveats listed in this section are resolved in Version 27.2. See Table 7 for the Cisco IOS software release that corresponds to the 27.2 microcode version.

- An Offload application uses up resources and prevents traffic from going through the port adapter on the 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 XCA major node failures. This failure occurs because VTAM overloads the PORT TIMER and, if the PORT TIMER is set too low, the 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'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 timeout. [CSCdj45782]

- The TN3270 Server crashes with fatal error code 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]
- 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 Channel Port Adapter (CPA). The channel interface is always up/up even if the physical interface cable is not attached to the CPA.

  There is no workaround.

  A new channel interface configuration command which is valid only for the CPA, **state-tracks-signal**, fixes this problem. This command directs the CPA's 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 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 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. If the mainframe offload application does not validate the offload message header buffer_length field and detect the ZERO length response data, it may 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 for this problem. 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 hsas-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: %CMCC: slot0 Out Lu 5.54: len=10,2C003601 00AE4B81 00C8
  *Apr 26 13:36:24: %CMCC: slot0 Out Lu 5.54: sna-state=8501,lu-flags=0D24D204
  *Apr 26 13:36:24: %CMCC: 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. Since the BID command was already received the server queues the AID frame:

  ```
  *Apr 26 13:36:24: %CMCC: slot0 In Tnet 212: len=13,00000100 42F7D7F5 11D7F5FF
       EF
  *Apr 26 13:36:24: %CMCC: 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: %CMCC: slot0 Out Lu 5.54: len=1484,2C003601 00AF0381
     80F10611 5D611DE8

*Apr 26 13:36:24: %CMCC: slot0 Out Lu 5.54: sna-state=8D01,lu-flags=0D24D204

*Apr 26 13:36:24: %CMCC: slot0 Out Tnet 212: len=1482,00000200 6C010411
     5D611DE8 40404040
```

— The client sends the response to the frame:

```
*Apr 26 13:36:24: %CMCC: slot0 In Tnet 212: len=8,02000000 6C00FFEF

*Apr 26 13:36:24: %CMCC: slot0 Out Lu 5.54: sna-state=8509,lu-flags=0B24D204

*Apr 26 13:36:24: %CMCC: slot0 In Lu 5.54: len=9,2C000136 00AF8381 00
```

— The BUG-inbound queued data was sent inbound before the EB command was received from the host:

```
*Apr 26 13:36:24: %CMCC: slot0 In Lu 5.54: len=15,2C000136 00200392 20F7D7F5
     11D7F5

*Apr 26 13:36:24: %CMCC: slot0 Out Lu 5.54: len=9,2C003601 00B00391 40
```

There is no workaround. [CSCdm31347]

- The TN3270 server LUs using LU Nailing fail. If a client IP address is nailed to an 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 [bad telnet connect]13[ipAddrClient]172.16.25.255:[tcpPortCl

%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]

Caveats for Version 27.0/Version 27.1 Modifications

This section describes possible unexpected behavior by Version 27.0. All the caveats listed in this section are resolved in Version 27.1. See Table 7 for the Cisco IOS software release that corresponds to the 27.1 microcode version.

- 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 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 intermittent fatal error (code=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]

- If a PCPA with 32 MB of memory is installed in a Cisco 7200 series router that has a Network Processing Engine (NPE) with 128 MB of memory, the PCPA will fail adapter diagnostics with the following messages:

```
%ADAPTER-0-DIAGFAIL: Port 0 failed the PCA Diagnostic Mode 1 diagnostic
%ADAPTER-0-DIAGDATA: Module Call: 0 0  Error ID: 0 F0000000
```

  A workaround is to change the Cisco 7200 series NPE memory to 64 MB or to replace the 32 MB of memory on the PCPA with 16 MB of memory. [CSCdm09617]

- 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]

CPA Microcode Release xcpa26 Caveats

The following section describes the caveats to current CPA microcode versions and the modifications made in current CPA microcode versions for xcpa26 microcode. The caveats listed apply to only the most serious problems. See Table 7 for the Cisco IOS software releases supported by xcpa26 microcode.

Caveats for Version 26.14/Version 26.15 Modifications

This section describes possible unexpected behavior by Version 26.14. All the caveats listed in this section are resolved in Version 26.15. See Table 7 for the Cisco IOS software release that corresponds to the 26.15 microcode version.

- 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 message number 9.

```
CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_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]

- The CMCC adapter fails with multiple fatal error messages (number 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]

Caveats for Version 26.13/Version 26.14 Modifications

This section describes possible unexpected behavior by Version 26.13. All the caveats listed in this section are resolved in Version 26.14. See Table 7 for the Cisco IOS software release that corresponds to the 26.14 microcode version.

- A user receives another user's 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 error message number 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 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 message number 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 message number 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 chain. The problem also may 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 may fail when the **shutdown** command is configured in TN3270 sub-mode.

  There is no workaround. [CSCdp99538]

- The CMCC adapter configured for CSNA may 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 message number 35:

  ```
  %CTA-0-INACTIVE: PA1 CTA 7C00-50 reset after being inactive for 180 seconds
  ```

  The workaround is to shutdown 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]

Caveats for Version 26.12/Version 26.13 Modifications

This section describes possible unexpected behavior by Version 26.12. All the caveats listed in this section are resolved in Version 26.13. See Table 7 for the Cisco IOS software release that corresponds to the 26.13 microcode version.

- 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 fatal error message number 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 can not 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 message number 32. This problem occurs when changing the IP address of a loopback interface.

  There is no workaround. [CSCdp85890]

Caveats for Version 26.11/Version 26.12 Modifications

This section describes possible unexpected behavior by Version 26.11. All the caveats listed in this section are resolved in Version 26.12. See Table 7 for the Cisco IOS software release that corresponds to the 26.12 microcode version.

- BADTIMER messages appear when running 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 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).
  ```

  [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:

  ```
  %CIP2-3-MSG: slot0 %SSI802-3-FATAL_ERROR: SSI_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 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]

- A print server with 10 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]

Caveats for Version 26.10/Version 26.11 Modifications

This section describes possible unexpected behavior by Version 26.10. All the caveats listed in this section are resolved in Version 26.11. See Table 7 for the Cisco IOS software release that corresponds to the 26.11 microcode version.

- 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. TheTN3270 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 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 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]

- 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 CMPC and CSNA, also.

  The workaround is to upgrade the 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 CMCC Adapter TN3270 server session. If the condition continues for another 2 minutes, the 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
  ```

  [CSCdm94788]

- 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]

- 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 CMCC adapter with TN3270 Server configured fails with fatal error message 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 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 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 CMCC Adapter configured for TCP/IP Offload fails with a 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]

Caveats for Version 26.9/Version 26.10 Modifications

This section describes possible unexpected behavior by Version 26.9. All the caveats listed in this section are resolved in Version 26.10. See Table 7 for the Cisco IOS software release that corresponds to the 26.10 microcode version.

- 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 CMCC TN3270 Server does not use this client IP address for matching on LU nailing statements in the configuration. [CSCdj44584]
- MSG10 data from one 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 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 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. TheTN3270 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 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 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 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]

- A user receives another user's 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 CMCC adapter fails with fatal error code 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 message code 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 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 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 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 non-structured 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 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]

Caveats for Version 26.8/Version 26.9 Modifications

This section describes possible unexpected behavior by Version 26.7. All the caveats listed in this section are resolved in Version 26.8. See Table 7 for the Cisco IOS software release that corresponds to the 26.8 microcode version.

- An Offload application uses up resources and prevents traffic from going through the port adapter on the 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 XCA major node failures. This failure occurs because VTAM overloads the PORT TIMER and, if the PORT TIMER is set too low, the 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'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 timeout. [CSCdj45782]

- The TN3270 Server crashes with fatal error code 35. See caveat CSCdk02535. 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]

- 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 CMCC.

[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 Channel Port Adapter (CPA). The channel interface is always up/up even if the physical interface cable is not attached to the CPA.

  There is no workaround.

  A new channel interface configuration command which is valid only for the CPA, **state-tracks-signal**, fixes this problem. This command directs the CPA's 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 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 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 CMCC to reload with fatal error message 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(xxxxxxxx) or index(92)

  Where "xxxxxxxx" 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 SESSEND.

  The workaround is to not use the SYSREQ key. [CSCdk83960]

- The CMCC Adapter running TN3270 fails with fatal error number 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]

- 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. If the mainframe offload application does not validate the offload message header buffer_length field and detect the ZERO length response data, it may 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 for this problem. 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 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]

- CMCC Adapter 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 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 00AECB81 00C8
  ```

  — An AID command is received before the host has a chance to send the BB command. Since 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
       EF

  *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 40404040
  ```

  — 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 00AF8381 00
  ```

— The BUG-inbound queued data was sent inbound before the EB command was received from the host:

```
*Apr 26 13:36:24:  %CIP: slot0 In Lu 5.54: len=15,2C000136 00200392 20F7D7F5
     11D7F5

*Apr 26 13:36:24:  %CIP: slot0 Out Lu 5.54: len=9,2C003601 00B00391 40
```

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. TheTN3270 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 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 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 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 CMCC Adapter 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 CMCC 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 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() may 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 re-open the server socket by restarting the server application on the host. [CSCdm63283]

Caveats for Version 26.7/Version 26.8 Modifications

This section describes possible unexpected behavior by Version 26.7. All the caveats listed in this section are resolved in Version 26.8. See Table 7 for the Cisco IOS software release that corresponds to the 26.8 microcode version.

- If a CIP2 PCA (Bus and Tag) has an Altera FLEX chip (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]

Caveats for Version 26.5/Version 26.7 Modifications

This section describes possible unexpected behavior by Version 26.5. All the caveats listed in this section are resolved in Version 26.7. See Table 7 for the Cisco IOS software release that corresponds to the 26.7 microcode version.

- If a PCPA with 32 MB of memory is installed in a Cisco 7200 series router that has a Network Processing Engine (NPE) with 128 MB of memory, the PCPA will fail adapter diagnostics with the following messages:

  ```
  %ADAPTER-0-DIAGFAIL: Port 0 failed the PCA Diagnostic Mode 1 diagnostic
  %ADAPTER-0-DIAGDATA: Module Call: 0 0  Error ID: 0 F0000000
  ```

  A workaround is to change the Cisco 7200 series NPE memory to 64 MB or to replace the 32 MB of memory on the PCPA with 16 MB of memory. [CSCdm09617]

- 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 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 intermittent fatal error (code=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 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 may 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 a 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 for this problem. This DDTS is a continuation of CSCdk86184. [CSCdm02126]

Caveats for Version 26.4/Version 26.5 Modifications

This section describes possible unexpected behavior by Version 26.4. All the caveats listed in this section are resolved in Version 26.5. See Table 7 for the Cisco IOS software release that corresponds to the 26.5 microcode version.

- Certain ESCON conditions lead to LOGDATA error messages that results 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 which 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. This workaround applies only for the CIP. [CSCdj61710]

- A print job hangs when printing through the 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 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 CMCC crashes with fatal error code 37 after the BSQ-0-SCB_CHAIN: Read SCB chain is out of sequence. If the routing processor sends an IP packet to the CMCC for a 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:

```
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 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 CMCC having the problem. [CSCdk41506]

- The CMCC adapter crashes with a fatal error code 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


  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#
  01:22:25: %SYS-5-CONFIG_I: Configured from console by console
  rispix#show ext ch 0/1 ip-stack
  ...No IP statistics found
  ```

  [CSCdk45042]

- The TCP connection is closed (FIN sent) before all data is sent. The remaining data (1 to 12 bytes) is sent after the connection is closed with FIN set again. 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 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, LU Type 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 Type 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]

Caveats for Version 26.2/Version 26.4 Modifications

This section describes possible unexpected behavior by Version 26.2. All the caveats listed in this section are resolved in Version 26.4. See Table 7 for the Cisco IOS software release that corresponds to the 26.4 microcode version.

- After shutting down the 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. [CSCdj78246]

- When running the 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 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]

- CMCC TN3270 Server's 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 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 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 will 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 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 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 LU, and that LU only became available within the last six 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 six seconds or to disconnect and reconnect immediately upon noticing the delay. [CSCdk28081]

- When using a logon manager through 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 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 CMCC TN3270 Server DLUR EN capability, connect to a logon manager such as NetView access or TPX. [CSCdk29362]

Caveats for Version 26.1/Version 26.2 Modifications

This section describes possible unexpected behavior by Version 26.1. All the caveats listed in this section are resolved in Version 26.2. See Table 7 for the Cisco IOS software release that corresponds to the 26.2 microcode version.

- When running CMCC TN3270 Server, the CMCC adapter reports fatal error code 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 may 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_FSM_ERR: TG Name: CMPCTG -CnlsLs, Event ITestInd, State SCnlsConnected
  %MBUF-0-MFREEx2: mfree: mbuf 845F0160 already free'ed 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 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]

- 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 may 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 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 CMCC TN3270 Server connects then disconnects a client. This occurs with LOGAPPL applications when the client sends data to the host application and the host's 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 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]
- 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 CMCC microcode reports a fatal error and reloads. This is an infrequent problem that occurs when there is a very small timing window. [CSCdk08533]
- Client disconnected when the host sent dactlu followed by actlu. In VTAM through cross domain, the host can send dactlu followed by actlu to clean up the lu session, but not to disconnect the lu session. [CSCdk08642]
- The CMCC microcode reports a fatal error and reloads. This 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 occurs either 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 shutdown or connected. [CSCdk09978]
- When the connection to a host from the CMCC TN3270 Server is not via the channel, data corruption may occur, resulting in bad XIDs or Binds being reported.

  There is no workaround. [CSCdk10071]
- 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'd LUs.

  The workaround is to locally clear the keyboard lock, if the client supports such a feature. Otherwise, the user must disconnect and reconnect. [CSCdk10200]
- The TN3270 Server refuses new TCP connections. This lasts for 2 to 20 minutes depending on the number of TCP requests. This occurs when there is one-way network congestion 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 and the client resends the SYN.

  There is no workaround. [CSCdk11113]
- When usingTN3270 Server to connect to NetView when the NetView type ahead feature is used, the lu-lu session can be stuck with a PROG MSG. Customer needs to recycle LU to continue.

  The workaround is to recycle the LU in VTAM and restart the session.[CSCdk11361]
- The CMCC adapter reports the IPC-NO-MEMD message and hangs. This occurs when CMCC adapter host communications have been cut off before a hierarchical reset. [CSCdk11787]
- CMCC TN3270 Server's DLUR session is unbound by DLUS with sense 1002 (RU length error) soon after the DLUR-DLUS pipe is established. This 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 locate which 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 was set on a RECV, RECVwait, or RECVwaitFORfin socket request, only the Offload message header and response header were returned to the host. The buffer length field in the Offload message header indicated MSG_PEEK data was present in the message but no data was 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 XCA node. [CSCdk14424]

Caveats for Version 26.0/Version 26.1 Modifications

This section describes possible unexpected behavior by Version 26.0. All the caveats listed in this section are resolved in Version 26.1. See Table 7 for the Cisco IOS software release that corresponds to the 26.1 microcode version.

- The CSNA responds to single router explorers with a specific router instead of an all routers explorer response. [CSCdi64614]
- After certain low memory conditions, 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]
- The CMCC Adapter reports a BSQ-x-SCB_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 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 timeout 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 may 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 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]

- 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 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's MVS TCPIP 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 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 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 CMCC adapter reports fatal error code 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 may occur when the maximum-lu limit has been reached or when no more 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 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 CMCC interface and then bringing it up again. [CSCdj80886]
- The CSNA responds to the TEST command when no SAP is active. This error may result in an end station trying to connect to a 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 may occur. [CSCdj80952]
- The 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 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 CMCC TN3270 server, the CMCC Adapter may sometimes report a Fatal error message (code=35) and spontaneously reload. [CSCdj81522]
- The CMCC microcode may 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]
- CSNA fails to send disconnect when indication buffer is in use. This causes the following results: the end-station is not able to 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 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 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 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 the 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 CMCC fatal error output report.This will help 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 CMCC DLUR repeatedly tries to establish CP-CP sessions with an incompatible NN server and fails to try other links for a NN server in the following conditions:

  — When using CMCC TN3270 server DLUR/DLUS with preferred-NNserver configured, when the DLUR is varied inactive by lu/cpname on the primary host and is defined statically on the primary, as cross-domain resource (CDRSC) or LU, but the link between the primary and the CMCC adapter is left active. This situation makes controlled SSCP takeover difficult.

  The workaround is to not configure preferred-NNserver. [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 CLAW protocol.

  There is no workaround. [CSCdj88636]

- 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 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]

- The CMCC TN3270 server command **show extended ch *x/2* tn3270 pu lu history** may cause the router to reload. This situation happens if the LU's 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 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 CMCC statements define the subchannels but for which there is no corresponding transmission group (TG) statement results in an unexpected reload.

  The workaround is to make sure the TG statement is configured before the associated CMCC statements. [CSCdk01922]

- The 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]

- 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 may 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 CMCC may 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 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 CMCC TN3270 Server is not via the channel, data corruption may occur, resulting in bad XIDs or Binds being reported.

  There is no workaround. [CSCdk10071]

CPA Microcode/Cisco IOS Software Compatibility Matrix

Table 7 lists the CPA microcode version and Cisco IOS software compatibility for the Cisco 7200 family.

Table 7 CPA Microcode Releases and Corresponding Cisco IOS Releases for the Cisco 7200 Family

Default CPA Microcode Version	Cisco IOS Release 11.3T	Cisco IOS Release 12.0	Cisco IOS Release 12.0T	Cisco IOS Release 12.1	Cisco IOS Release 12.1T
xcpa26-0	11.3(3) T				
xcpa26-1	11.3(4)T				

Table 7 CPA Microcode Releases and Corresponding Cisco IOS Releases for the Cisco 7200 Family (continued)

Default CPA Microcode Version	Cisco IOS Release 11.3T	Cisco IOS Release 12.0	Cisco IOS Release 12.0T	Cisco IOS Release 12.1	Cisco IOS Release 12.1T
xcpa26-2	11.3(5)T, 11.3(6)T				
xcpa26-4	11.3(7)T	12.0(1), 12.0(2)	12.0(1)T, 12.0(2)T		
xcpa26-5	11.3(8)T	12.0(3)			
xcpa26-7	11.3(9)T	12.0(4)			
xcpa26-8	11.3(10)T, 11.3(11)T	12.0(5)			
xcpa26-9		12.0(6), 12.0(7)			
xcpa26-10		12.0(8)			
xcpa26-11		12.0(9)			
xcpa26-12		12.0(10)			
xcpa26-13		12.0(11)			
xcpa26-15		12.0(12)			
xcpa26-16		12.0(13)			
xcpa26-17		12.0(14)			
xcpa26-18		12.0(15)			
xcpa26-20		12.0(16)			
xcpa27-0			12.0(3)T		
xcpa27-1			12.0(4)T		
xcpa27-2			12.0(5)T		
xcpa27-4			12.0(7)T		
xcpa27-6				12.1(1)	12.1(1)T
xcpa27-7				12.1(2)	12.1(2)T
xcpa27-8				12.1(3)	12.1(3)T
xcpa27-9				12.1(4)	
xcpa27-11				12.1(6)	
xcpa27-13				12.1(7)	
xcpa28-1					12.1(5)T

Caution With microcode levels prior to xcpa26-7, the PCPA will fail adapter diagnostics when the PCPA has 32 MB of memory and is installed in a Cisco 7200 series router that has a Network Processing Engine (NPE) with 128 MB of memory. Possible workarounds include upgrading to microcode versions xcpa26-7, or changing the Cisco 7200 series NPE memory to 64 MB or replacing the 32 MB of memory on the PCPA with 16 MB of memory.

CPA-Related Caveats for Cisco IOS Releases

For a complete list of caveats against the Cisco IOS Releases, use Cisco Documentation CD-ROM or access Cisco Connection Online as described in the section “Cisco Connection Online” later in this document. You can also refer to the following publications, which are available on Cisco Connection Documentation:

- *Release Notes for Cisco IOS Release 11.3* (Document Number 78-4998-xx)
- *Release Notes for Cisco 7000 Family for Cisco IOS Release 11.3T* (Document Number 78-5015-xx)
- *Release Notes for Cisco IOS Release 12.0* (Document Number 78-6035-xx)
- *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0T* (Document Number 78-6055-xx)
- *Release Notes for Cisco IOS Release 12.1* (Document Number 78-10724-xx)
- *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.1T* (Document Number 78-10811-xx)

CPA and Processor Module ROM Monitor Recommendations

CPA and Cisco 7200 series ROM monitor (system bootstrap) versions and system software images are typically independent of each other; however, the CPA hardware version does have minimum requirements in terms of Cisco IOS release and CPA microcode version as listed in Table 8. Other microcode versions can be used, but only when specifically instructed to do so by technical support personnel. Table 9 identifies the processor module monitor versions.

Use the **show diag** EXEC command to display the CPA hardware version. The CPA card is identified as version 1.0.

Table 8 CPA Hardware, Cisco IOS Release, and CPA Microcode Compatibility

CPA Hardware Version	Minimum Cisco IOS Release Required	Minimum CPA Microcode Version Recommended
ESCON Channel Port Adapter	11.3(3)T	xcpa26.0
	12.0(1)	xcpa26.4
	12.0(1)T	xcpa26.4
Parallel Channel Port Adapter	11.3(9)T	xcpa26.7
	12.0(4)	xcpa26.7
	12.0(3)T	xcpa27.0
	12.1(1)	xcpa27.6
	12.1(1)T	xcpa27.6

Table 9 Minimum Recommended CPA Boot ROM Versions

Platform and Processor	Processor ROM Monitor Version
Cisco 7200 router	System Bootstrap Version 11.1 CA or later

CPA and Cisco 7200 DRAM Requirements

For the Cisco routers to take advantage of the Cisco IOS release CPA features, you might need to upgrade code, main system, or CPA memory. For specific Cisco IOS-related memory requirements, refer to the *Release Notes for Cisco 7000 Family for Cisco IOS Release 11.3T,* the *Release Notes for Cisco IOS Release 12.0(x),* the *Release Notes for Cisco IOS Release 12.0(x)T,* the *Release Notes for Cisco IOS Release 12.1(x),* or the *Release Notes for Cisco IOS Release 12.1(x)T* publication which is available on Cisco Connection Online.

CPA Microcode Upgrade Overview

To upgrade CPA microcode, complete the following steps.

Note You must be running Cisco IOS Release 11.3(3)T or later to complete the following steps.

Caution With microcode levels prior to xcpa26-7, the PCPA will fail adapter diagnostics when the PCPA has 32 MB of memory and is installed in a Cisco 7200 series router that has a Network Processing Engine (NPE) with 128 MB of memory. Possible workarounds include upgrading to microcode versions xcpa26-7, or changing the Cisco 7200 series NPE memory to 64 MB or replacing the 32 MB of memory on the PCPA with 16 MB of memory.

Upgrading from CCO

To upgrade to CPA microcode images obtained from CCO, do the following:

Step 1 Download the CPA microcode image from CCO to a TFTP server.

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

Step 3 Copy the CPA 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 4 Reconfigure the router, as necessary, to use the CPA microcode image 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 Save your running configuration to a TFTP server or Flash memory or SanDisk memory device.

Step 6 Perform a microcode reload.

For more detailed information on upgrading the CPA microcode image, refer to the *PA-1C-E ESCON Channel Port Adapter Installation and Configuration* note and the *PA-1C-P Parallel Channel Port Adapter Installation and Configuration* note.

Cisco Connection Online

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

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

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

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

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

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the *Release Notes for Cisco IOS Release 11.3*, *Release Notes for Cisco 7000 Family for Cisco IOS Release 11.3T*, *Release Notes for Cisco IOS Release 12.0*, *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0T*, *Release Notes for Cisco IOS Release 12.1* and the *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.1T* publications.