

Causes of CMCC-3-IPCDNSFAIL and CMCC-5-IPCDNSQUERYTIMEDOUT Error Messages

Document ID: 28361

Introduction

Prerequisites

Requirements

Components Used

Conventions

Inverse Domain Name System (DNS) Nailing

%CMCC-3-IPCDNSFAIL: DNS lookup failed and

%CMCC-5-IPCDNSQUERYTIMEDOUT: Error Messages

Solution for Reason #1

Solution for Reason #2

Related Information

Introduction

This document explains the causes of %CMCC-5-IPCDNSQUERYTIMEDOUT: and %CMCC-3-IPCDNSFAIL: error messages. You can encounter these error messages on Cisco 7200 and Cisco 7500 Series Routers that have these versions of hardware microcode on the Channel Interface Processor (CIP) and Channel Port Adapter (CPA) in Cisco IOS® Software Release 12.1(5)T and later:

- CIP hardware microcode CIP28-1 and later
- CPA hardware microcode xCPA28-1 and later

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.1(5)T and later
- Cisco 7200 and Cisco 7500 Series Routers
- CIP hardware microcode CIP28-1 and later
- CPA hardware microcode xCPA28-1 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Inverse Domain Name System (DNS) Nailing

The Inverse DNS Nailing enhancement enables the TN3270 server to nail a pool of logical units (LUs) to client machine names or to an entire domain. This enhancement allows dynamic IP addressing on the TN3270 client machines. This addressing is used in network design scenarios, such as a Dynamic Host Configuration Protocol (DHCP) environment and in individual network configuration scenarios, for example, when a machine is moved and needs a new network address.

The Inverse DNS Nailing enhancement was first introduced as a TN3270 Server Connectivity Enhancement feature on the CIP and CPA in Cisco IOS Software Release 12.1(5)T, and is applicable for:

- CIP hardware microcode CIP28–1 and later
- CPA hardware microcode XCPA28–1 and later

The Cisco IOS software inverse nailing support uses the DNS in routers to look up the symbolic name associated with a client IP address. The TN3270 server uses this symbolic name to assign a predefined LU pool for the user, and thus eliminates the need for nailed TN3270 clients to have statically–defined IP addresses. If you configure inverse DNS nailing on the TN3270 server, you do not need to modify the DNS nailing statements in the router configuration.

To use inverse DNS nailing on the TN3270 server, you must specify which DNS servers are required to resolve the TN3270 server client IP addresses. To specify the DNS servers, use these router commands:

- **ip domain–lookup**
- **ip domain–name**
- **ip name–server**

For additional information about the Inverse DNS Nailing feature, refer to the "Restrictions" section of TN3270 Server Connectivity Enhancements.

%CMCC–3–IPCDNSFAIL: DNS lookup failed and %CMCC–5–IPCDNSQUERYTIMEDOUT: Error Messages

The `CMCC–3–IPCDNSFAIL` error message is the result of an inverse DNS Nailing feature on the TN3270 Server. If this feature is *not* currently in use and if you have these versions of hardware microcode on the CIP and CPA in Cisco IOS Software Release 12.1(5)T or later:

- CIP hardware microcode between CIP28–7 (including CIP28–7) and CIP28–1
- CPA hardware microcode between xCPA28–7 (including xCPA28–7) and xCPA28–1

There are two possible reasons for this error message:

- Reason #1 You have not disabled the DNS and this error message is logged to the console or router log:

```
%CMCC-5-IPCDNSQUERYTIMEDOUT: DNS lookup failed - query to DNS server 0.0.0.0 timed o
```

- Reason #2 The DNS is disabled with the **no ip domain–lookup** command and this error message is logged to the console or router log:

Solution for Reason #1

A noticeable delay occurs when the client connects, and this results in a DNS failure logged. These issues occur when configured DNS servers are unreachable, or when a client IP address cannot be found and causes a search through multiple servers or a retry of DNS servers. When you do not use the inverse DNS Nailing feature, code should not check the DNS servers. This problem has been fixed in DDTs CSCdu88459, and the fix has been integrated in CIP28-8 and xCPA28-8.

The workaround is to ensure that DNS servers are reachable and DNS names are defined when DNS servers are configured. Configure the server with the **no ip domain-lookup** command to prevent delays. However, this does not prevent the DNS lookup failures from being logged.

Solution for Reason #2

DNS has been disabled with the **no ip domain-lookup** command, but in the router log CMCC-3-IPCDNSFAIL: DNS lookup failed messages are logged in every connection to TN3270 servers.

Between 28-7 and 28-1 hardware microcode levels, code checks the DNS Server by default when TN3270 is configured without the inverse DNS Nailing feature checked. After the fix for CSCdu88459, the IP address of the DNS server is checked if the inverse DNS Nailing feature has been enabled in the TN3270 server. If you do not want to see CMCC-3-IPCDNSFAIL: DNS lookup failed messages, you can suppress the message log, or you can make a CIP or xCPA hardware microcode upgrade to 28-8 or later.

You can download the CIP and xCPA microcodes from the Cisco Software Center (registered customers only) .

Related Information

- [TN3270 Server Connectivity Enhancements](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 11, 2005

Document ID: 28361
