Release Notes for Cisco LocalDirector Version 4.2.5

May 14, 2003

Note The most current Cisco documentation for released products is available on Cisco.com at http://www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Contents

This release note contains the following sections:

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

Open Caveats in LocalDirector Software Version 4.2.5

The following caveats are open in LocalDirector software version 4.2.5:

- **CSCeb01501** - The Local Director generates a non-standard HEAD request when using an HTTP probe to validate the activity of real servers. The HEAD request initiated by the LocalDirector may include an additional whitespace character before the User-Agent line in the HTTP header. The additional whitespace character may cause some Web servers to generate an error message.
- **CSCdy37648** - For defined UDP static translations, LocalDirector does not translate fragmented packets.
- **CSCea71603** - You can configure the LocalDirector to perform a static NAT of multiple real server IP addresses to a single virtual server IP address for TCP traffic using the **static** command. However, in this configuration, the LocalDirector software also NATs the ICMP echo (ping) initiated by the real server outside the LocalDirector, and the response does not correctly NAT back to the real server. As a result, a ping from each of the real servers to the other side of the LocalDirector fails. The only real server that has ICMP traffic NATed correctly is the last real server added to the static list.

  For example, in the scenario below, only the real server at IP address 4.4.4.4 in the static list has the correct NATing of ICMP frames. The other real servers, at IP address 2.2.2.2 and 3.3.3.3, do not.

  ```
  virtual 1.1.1.1
  real 2.2.2.2
  real 3.3.3.3
  real 4.4.4.4

  static 1.1.1.1 2.2.2.2
  static 1.1.1.1 3.3.3.3
  static 1.1.1.1 4.4.4.4
  ```

  To resolve this condition, use the **static** command to translate only a single real server IP address to that of a virtual server. For example:

  ```
  virtual 1.1.1.1
  virtual 1.1.1.2
  virtual 1.1.1.3
  real 2.2.2.2
  real 3.3.3.3
  real 4.4.4.4

  static 1.1.1.1 2.2.2.2
  static 1.1.1.2 3.3.3.3
  static 1.1.1.3 4.4.4.4
  ```

Resolved Caveats in LocalDirector Software Version 4.2.5

The following caveats were resolved in LocalDirector software version 4.2.5:

- **CSCea16571** - Local Director Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers. This vulnerability is present in all released versions. It affects only the security of TCP connections that originate or terminate on the Local Director device itself; it does not apply to TCP traffic forwarded through the device in transit between other hosts. To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. Workarounds for this vulnerability include strictly limiting permitted management hosts, and installation of anti-spoofing filters on the network perimeter of the installation site.

  This advisory is available at http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml.

- **CSCea00483** - Entering the letter "u" from a Telnet session and then closing the session without properly logging out causes the LocalDirector to reboot.
- **CSCdx07160** - When you enable the primary and secondary LocalDirector units for both stateful failover and the sticky feature, and enable spanning tree on the LocalDirector ports, a system reboot may cause the primary active LocalDirector to failover. The new active LocalDirector unit sends HTTP requests to a different server for approximately 30 seconds after booting up the primary LocalDirector. To resolve this issue, change the switch configuration in your network to disable spanning tree.
- **CSCdz08134** - The Telnet and Enable passwords are not case-sensitive. For example, a password of "cisco" and "Cisco" are considered to be the same by the LocalDirector software.
- **CSCdy08259** - With the **reassign** command set to a value of **2**, the LocalDirector does not reassign a new server until the fourth TCP SYN packet fails to get a response for the same connection. LocalDirector should reassign a server on receipt of the third TCP SYN packet. The default is three TCP SYN packets. After the third packet receives no response or a TCP RST from the server, the fourth packet is sent to another server.
- **CSCdz09473** - If you set up a static association using the **static** command without a corresponding real server, the LocalDirector may time out the connection prematurely. Having a static association set up without a specified real server results in a failure of the Local Director software to fill in the proper timeout value. This may cause the LocalDirector's cleanup thread to prematurely remove the connection upon the first inspection, which times out the connection prematurely.

  If you define a real server with the static association, then this issue should not occur. LocalDirector uses the real server's timeout value and clears the connection.
- **CSCdx13773** - When using the **sticky generic** command (but not the **sticky ssl** command) to connect to the same real server, occasionally an SSL session hangs. In this case, when the SSL session is about to end, the LocalDirector sends a TCP RST (reset) to the client, but not to the real server. The next time the same client (source address) establishes a new connection with a new source port to the same VIP on the Local Director, the LocalDirector sends the request to the same server. The server considers the new connection to be the same as the old connection. After a number of unsuccessful attempts, the LocalDirector tries another server, without marking the first server as Failed. As a result, the client application terminates.
- **CSCdy16810** - When using the LocalDirector in sticky cookie-insert mode, the day of the week listed in the cookie expiration time is not RFC-compliant.
- **CSCdy16926** - LocalDirector generates traps with conflicting information for version and protocol data unit (PDU) type. This may cause problems for network management applications because the trap does not get processed or is processed improperly, depending on the application behavior. There is no workaround to this issue.
- **CSCdv21441** - When using the Linux **snmpwalk** utility to walk through the LocalDirector MIBs, the MIB variable cldexVirtualTotalBytes does not properly list all the virtual servers configured on the device.
- **CSCdz23459** - The *Cisco LocalDirector Configuration and Command Reference Guide* incorrectly states that the **buddy** command has no limitations for the number of buddy associations configurable configured in the LocalDirector software. For LocalDirector version 4.2.4, the **buddy** command has a limitation of 64 buddy associations. With LocalDirector version 4.2.5, the maximum number of buddy associations is increased from 64 to 1024.
- **CSCdy29124** - When the cookie value for a real server is smaller than a previous cookie value, LocalDirector leaves additional characters at the end of the cookie value for the value that was previously stored in the sticky cookie association. The additional characters can cause the sticky connection, based on a cookie created by LocalDirector, to expire.

- **CSCea32446** - During a TCP flow connection, Local Director model LD417 may identify a bad TCP checksum and drop the received packets. This incorrect identification of a bad TCP checksum typically occurs in any LocalDirector with an Intel i82559 Rev 8 Network Interface Card (included by default in LocalDirector model LD417). The packets, however, do not have a bad TCP checksum; the checksum is computed incorrectly. To check the revision of the installed Network Interface Card in the LocalDirector, use the **show interface** CLI command.
- **CSCdy32975** - A LocalDirector configured for HTTP probe support occasionally uses source TCP ports below 1024. This can trigger a warning on Intrusion detection systems when a TCP port assigned to another application is used.
- **CSCea37475** - The LocalDirector software allows you to specify a configuration so that any host, on any network, can Telnet to the LocalDirector. In some cases, access to LocalDirector does not work with the command **telnet 0.0.0.0 0.0.0.0**. The workaround to this issue is to specify a host address as shown below to allow access from any hosts at any network.

  ```
  telnet 255.0.0.0 0.0.0.0
  telnet 10.0.0.0 0.0.0.0
  ```

- **CSCdy37674** - For UDP static translations, the UDP real server must be defined for packets to flow.
- **CSCdz39957** - The LocalDirector occasionally reboots due to the receipt of a corrupt stateful connection replication message on the Standby unit.
- **CSCdm62909** - When using the Linux **snmpwalk** utility, the GET NEXT request fails to fully search the MIB nodes in lexicographical order when starting at some nonleaf nodes. Use the **snmpwalk** utility to search the entire tree.
- **CSCdx71253** - SSL sticky does not work for connections where the SSL client and SSL server have previously negotiated a SSL session ID but the LocalDirector does not contain the SSL session ID in its tables.
- **CSCdz75386** - Adds the **arp retries** command to adjust the behavior of the ARP subsystem in LocalDirector. This command adjusts the frequency and number of times that LocalDirector attempts to perform an ARP for a destination IP address. See the **arp retries** command in the "New Command in LocalDirector Software Version 4.2.5" section.
- **CSCdy76817** - The LocalDirector may reboot when a real server contains a static definition on the LocalDirector and that same real server is load-balancing FTP traffic.
- **CSCdz77135** - The LocalDirector software does not time out dynamic ARP table entries after exceeding the time period specified using the **arp timeout** *seconds* command. In this case, LocalDirector eventually times out dynamic ARP table entries after exceeding approximately two times the specified timeout value.
- **CSCdz77227** - If the LocalDirector has a valid ARP entry, but does not have an entry in its bridge table, the packets for that destination are sent out all LocalDirector interfaces.
- **CSCdz79776** - The Standby LocalDirector interface remains stuck in Testing mode during failover interface setup. Each LocalDirector maintains its own copy of the interface status for both boxes. In this case, one LocalDirector may incorrectly show that the other unit is in Testing mode. In many cases, the second LocalDirector is not in Testing mode and is functioning normally.
- **CSCdz81907** - In proxy mode for content load-balancing, the LocalDirector appears to not complete the 3-way TCP handshake on approximately 20 percent of the connections. This issue relates to the LocalDirector incorrectly identifying when a content rule had been matched. After a match for the content rule occurs and the other data packets arrive, LocalDirector should then send a TCP RST handshake to terminate the connection.
- **CSCdy85450** - Removing a virtual server with a bind ID may sometimes cause other virtual servers sharing the same IP address to fail.

- **CSCdz86881** - LocalDirector fails to process an HTTP GET request with a 1033 byte URL string and then resets the connection. This issue can occur under the following conditions:
  - LocalDirector spoofs client connection to inspect a cookie.
  - The URL spans two packets due to a TCP maximum segment size of 1024 bytes from the transmitting device.
- **CSCdz87139** - The LocalDirector intermittently reboots due to the general housekeeping that occurs within the appliance when a real server fails due to it becoming nonresponsive to new connections. When this happens, the LocalDirector first clears all buddy sticky associations that the real server may have (this is only done if the virtual server is in a buddy group). LocalDirector then generates a syslog message, which is sent to a syslog host if one is defined or has been added to the internal circular buffer. The LocalDirector reboot occurs between these two processes.

New Command in LocalDirector Software Version 4.2.5

Table 1 lists the command and options that has been added to software version 4.2.5.

Table 1 Commands and Options Added to Version 4.2.5

Mode	Command and Syntax	Description
Privileged, configuration	**arp retries** *seconds num*	Adjusts the behavior of the ARP subsystem in LocalDirector. This command adjusts the frequency and number of times that LocalDirector attempts to perform an ARP for a destination IP address. The options for this command include: • *seconds* - The frequency that LocalDirector performs an ARP for the destination IP address. Valid entries are 1 to 2000000 seconds. The default is 15 seconds. • *num* - The number of times that LocalDirector performs an ARP for a destination IP address range of values. Valid entries are 4 to 50. The default is 4. For example, in the configuration below, LocalDirector will transmit an ARP request every two seconds, sending a total of 50 ARP requests, before it stops sending ARP requests. `arp retries 2 50`

Related Documentation

The following documents provide additional information and should be used in conjunction with these release notes:

- *Cisco LocalDirector Configuration and Command Reference Guide, Version 4.2*
- *Cisco LocalDirector Hardware Installation Guide*
- *Cisco LocalDirector 417 Hardware Installation Guide*
- *Release Notes for Cisco LocalDirector 417G*
- *Regulatory Compliance and Safety Information for Cisco LocalDirector*
- *Cisco Content Router 4400 User Guide*

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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