CISCO SYSTEMS

®

Text Part Number: 78-4176-20 Rev. C0

Release Notes for Cisco DistributedDirector System Software

February 24, 2002

Introduction

These release notes describe the features and caveats for Cisco DistributedDirector System Software (Cisco IOS Release 11.1 IA), beginning with Release 11.1(9)IA, up to and including Release 11.1(28)IA2.

These release notes discuss the following topics:

- Documentation, page 2

- Platform Support, page 2

- Cisco IOS Packaging, page 3

- Memory Requirements, page 3

- New Features in Release 11.1(28)IA

- New Features in Release 11.1(25)IA, page 4

- New Features in Release 11.1(18)IA, page 5

- Important Notes, page 5

- Release 11.1(28)IA1 Caveats, page 6

- Release 11.1(28)IA Caveats, page 9

- Release 11.1(27)IA Caveats/Release 11.1(28)IA Modifications, page 9

- Release 11.1(26)IA Caveats/Release 11.1(27)IA Modifications, page 10

- Release 11.1(25)IA Caveats/Release 11.1(26)IA Modifications, page 10

- Release 11.1(24)IA Caveats/Release 11.1(25)IA Modifications, page 10

- Release 11.1(23)IA Caveats/Release 11.1(24)IA Modifications, page 11

- Release 11.1(22)IA Caveats/Release 11.1(23)IA Modifications, page 11

Documentation

Cisco DistributedDirector documentation is a combined installation and configuration guide for DistributedDirector hardware. Functionality specific to Cisco DistributedDirector System Software is included in the configuration chapters in the following publications:

- *Cisco DistributedDirector 2500 Series Installation and Configuration Guide*
- *Cisco DistributedDirector 4700-M Installation and Configuration Guide*

These documents are available as printed manuals or electronic documents at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/index.htm

---

Note The Documentation CD-ROM contains DistributedDirector documentation beginning with the March 1997 version. Electronic documents are available from Cisco Connection Online, as described in the section "Cisco Connection Online" later in this document.

Platform Support

Cisco DistributedDirector System Software (Release 11.1 IA) supports the following platforms:

- Cisco DistributedDirector 2501
- Cisco DistributedDirector 2502
- Cisco DistributedDirector 4700-M

Table 1 summarizes the LAN interfaces supported on each platform.

Table 1   LAN Interfaces Supported by Cisco DistributedDirector Platforms

Interface	DistributedDirector 2501	DistributedDirector 2502	DistributedDirector 4700-M
Ethernet (AUI)	Yes	No	Yes
Ethernet (10BaseT)	No	No	Yes
Fast Ethernet (100BaseTX)	No	No	Yes
Fast Ethernet (100BaseT4)	No	No	Yes
4-Mbps Token Ring	No	Yes	Yes
16-Mbps Token Ring	No	Yes	Yes
FDDI Multimode DAS	No	No	Yes

Cisco IOS Packaging

One feature set (image) is available for each DistributedDirector platform.

Note   No routing functionality is supported in Cisco DistributedDirector System Software images.

Memory Requirements

Table 2 shows memory requirements for the Cisco DistributedDirector Sets.

Table 2   Release 11.1 IA Memory Requirements

Router	Minimum Required Code Memory	Required Main Memory	Release 11.1 IA Runs from
Cisco DistributedDirector 2501	8 MB Flash	8 MB RAM	Flash
Cisco DistributedDirector 2502	8 MB Flash	8 MB RAM	Flash
Cisco DistributedDirector 4700-M	16 MB Flash	32 MB RAM	RAM

New Features in Release 11.1(28)IA

Cisco DistributedDirector Enhancements for Release 11.1(28)IA
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/ddenh3.htm

The DistributedDirector now supports the following three new features:

- Enhanced Fault Tolerance with Multiple Resource Records
- Critical Event Recording with Syslog
- Enhanced Server Verification with Multiple Port Connect Test

Note   These new features are currently only supported in Cisco IOS Release 11.1(28)IA. They will be included in Cisco IOS Release 12.1(3)T and subsequent 12.1 T releases.

Enhanced Fault Tolerance with Multiple Resource Records

Prior to this enhancement, DistributedDirector would return a single Resource Record (RR) in each DNS response. This was normally sufficient, but for some applications, server failover will occur more rapidly when applications are provided IP addresses of multiple servers.

The Enhanced Fault Tolerance with Multiple Resource Records feature enables DistributedDirector to return multiple RR. The number of RR returned in a single reply is configurable. The default number of RR returned is one.

Critical Event Recording with Syslog

The Critical Event Recording with Syslog feature enables DistributedDirector to log critical events by way of the industry-standard syslog system. Server state is logged, providing a useful log of when servers are considered up or down. Additionally, the server selection process may be logged. In both cases, the logging priority level is "informational."

Enhanced Server Verification with Multiple Port Connect Test

Prior to this enhancement, DistributedDirector could evaluate server status by performing a TCP connect test to a single port. The Enhanced Server Verification with Multiple Port Connect Test feature allows multiple connect ports to be specified. If any one of the connect tests fail, the server is considered down.

New Features in Release 11.1(25)IA

Cisco DistributedDirector Enhancements for Release 11.1(25)IA
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/ddenh2.htm

The DistributedDirector now supports the following four new features:

- Support for DNS Mail Exchange Records
- Policy Redirection
- Unlimited Number of IP Addresses Per Virtual Hostname
- Per-Hostname Time-to-Live

Support for DNS Mail Exchange Records

The Support for Domain Name System (DNS) Mail Exchange (MX) Records feature enables transparent global load distribution of Simple Mail Transfer Protocol (SMTP)-based e-mail services. This enables Cisco DistributedDirector to redirect client e-mail requests to the best SMTP server by way of a single DNS MX Resource Record. Cisco DistributedDirector then sends a single DNS MX resource record to the client that identifies the best available SMTP server. Cisco DistributedDirector can use all of its decision-making metrics to determine the best SMTP server for a client request.

Policy Redirection

The Policy Redirection feature enables the Cisco DistributedDirector to direct IP services to a single server or distribute IP service requests across a subset of servers based on IP address and mask. This feature also introduces special access control lists (ACLs) that identify a set of servers to be used for queries for a specific DistributedDirector host name.

Unlimited Number of IP Addresses Per Virtual Hostname

The Unlimited Number of IP Addresses Per Virtual Hostname feature enables the Cisco DistributedDirector to support an unlimited number of IP addresses per virtual host name. Previously, each virtual host name could only support a maximum of eight IP addresses.

Per-Hostname Time-to-Live

The Per-Hostname Time-to-Live (TTL) feature enables Cisco DistributedDirector to configure the TTL values of its Domain Name System (DNS) resource records. Each virtual host name can have a unique TTL configuration. This feature applies only to address and mail exchange resource records generate by Cisco DistributedDirector—not resource records relayed from a forwarding server through Cisco DistributedDirector.

New Features in Release 11.1(18)IA

Cisco DistributedDirector Enhancements for Release 11.1(18)IA

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/ddenh.htm

The DistributedDirector and Director Response Protocol (DRP) now support additional traffic redirection criteria. In addition to making redirection decisions based on client-to-server topological proximity using DRP, random distribution, and administrative preferences, the DistributedDirector now supports the DRP-MED option, the DRP-RTT metric, the "portion" metric, and the DRP-RTT Tolerance parameter.

Important Notes

This section describes important information about using the Cisco IOS Release 11.1 IA software.

- Director Response Protocol (DRP) server agent support (which is enabled on a Cisco router) is available in Cisco IOS Releases 11.3 and 11.3 T. Use of DistributedDirector System Software Release 11.1(18)IA and later requires the use of DRP agent support in Release 11.3(2)T and later (if DRP is used).

Release 11.1(28)IA2 Caveats

Cisco IOS Release 11.1(28)IA2 is a rebuild release for Cisco IOS Release 11.1(28)IA. The caveats in this section are resolved in Cisco IOS Release 11.1(28)IA2 but may be open in previous Cisco IOS releases.

- CSCdw78210

Related to fixes in CSCdw65903 and outlined in:

http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml.

This defect may be seen when "debug snmp packets" is turned on and can result in tracebacks.

Release 11.1(28)IA1 Caveats

Cisco IOS Release 11.1(28)IA1 is a rebuild release for Cisco IOS Release 11.1(28)IA. The caveats in this section are resolved in Cisco IOS Release 11.1(28)IA1 but may be open in previous Cisco IOS releases.

- CSCdp11863

  Cisco IOS software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as "sysContact", "sysLocation", and "sysName", that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

  The vulnerability is only present in certain combinations of IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every IOS release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

  To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

  In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or "*ilmi" view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

  This notice will be posted at http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml.

- CSCdp50574

  DistributedDirector may not distribute requests properly per the portion metric that is configured. For example, server 1 has a portion metric of 3 and server 2 has a portion metric 7. When 100 queries are sent, server 1 receives 31 queries and server 2 receives 69 queries. There is no workaround.

- CSCdr17862

  DistributedDirector may not automatically learn when a server is removed from a host name and may try to use the configuration for a server that has already been deleted. There is no workaround.

- CSCdr26416

  DistributedDirector may experience random reloads if incomplete cache entries were created when no servers were available for selection. There is no workaround.

- CSCdr36952

A defect in multiple versions of Cisco IOS software will cause a Cisco router or switch to stop and reload if the Cisco IOS http service is enabled and an attempt is made to browse to http://<router-ip>/%%. This defect can be exploited to produce a denial of service (DoS) attack. This defect has been discussed on public mailing lists and should be considered public information.

The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS Release 11.1 through Release 12.1. The vulnerability has been corrected and Cisco is making fixed versions available to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect.

Workaround: Nullify the vulnerability by disabling the Cisco IOS HTTP server, by preventing access to the port in use by the HTTP server on the affected router or switch, or by applying an access-class option to the service itself. The IOS HTTP server is not enabled by default except on a small number of router models in specific circumstances.

Please see http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml for the latest complete version of this security advisory.

- CSCdr57740

When DistributedDirector relays Domain Name System (DNS) answers from another backend DNS server, DistributedDirector may return only one answer record even if the backend DNS server returns multiple answer records. There is no workaround.

- CSCdr65238

When DistributedDirector exchanges a Director Response Protocol (DRP) packet with a DRP agent, DistributedDirector may reload and reboot. There is no workaround.

- CSCdr80330

DistributedDirector may redistribute requests unevenly. There is no workaround.

- CSCdr80887

While running Open Shortest Path First (OSPF) protocol with a heavy Domain Name System (DNS) query load (for example, three DNS clients each sending 400-packets per second [pps]), DistributedDirector may reload with a bus error. There is no workaround.

- CSCds04747

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml.

- CSCds13630

When multiple hostnames are configured on the same pair of servers, the portion metric may not be allocated correctly. The actual ratio of hits against assignments is off the mark. This condition has been observed when two or more hosts share the same servers.

Workaround: Assign multiple IP addresses to a shared server so that each sharing host may use a different IP address for this server.

- CSCds14291

  DistributedDirector may reload when a server is removed. There is no workaround.

- CSCds41469

  The help string for the **ip director default-weights** [**drp-rtt**] global configuration command may be incorrectly displayed as "Weight for drp server metric" instead of "Weight for drp rtt metric".

- CSCds41863

  The Cisco IOS Domain Name System (DNS) server will send an authoritative reply when a DNS A record is configured instead of a DNS Start of Authority (SOA) record. This configuration is not recommended. There is no workaround.

- CSCds51433

  When Syslog is turned on with **ip dir host** *hostname* **logging** global configuration command, the show command **show ip dir host** does not show that Syslog is turned on. There is no workaround.

- CSCds58605

  A server configuration may be deleted automatically if it is not associated with any host, and only port-specific information is configured for the server.

  Workaround: Associate servers with hosts by entering the **ip host** *host servers* command.

- CSCds66165

  When DistributedDirector has only one server for a host name, it may not show the number of times the server has been advertised. There is no workaround.

- CSCds66588

  A memory leak may occur under various timing conditions when a backend name server is used with DistributedDirector. There is no workaround.

- CSCds69266

  The Cisco IOS Domain Name System (DNS) server does not process a Start Of Authority (SOA) record configuration correctly in some cases. When an SOA record is configured with the **ip dns primary** command, the DNS server will only be authoritative for that domain name and those one level below that domain. For example, given

  ip host *x.foo.com ...*
  ip host *x.x.foo.com ...*
  ip dns primary *foo.com soa ...*

  the DNS server will be authoritative for *x.foo.com* but will not be authoritative for *x.x.foo.com*.

  Workaround: Configure an SOA for every two levels of DNS hierarchy. For example:

  ip host *x.foo.com ...*
  ip host *x.x.foo.com ...*
  ip dns primary *foo.com soa ...*
  ip dns primary *x.x.foo.com soa ...*

- CSCds69316

DistributedDirector may reload when a host or server is removed automatically, and the host or server is still referenced. There is no workaround.

- CSCds86028

    The maximum time-to-live (TTL) for a resource record in DistributedDocument is 43200 seconds, which is half a day. There is no workaround.

- CSCds91873

    DistributedDirector reloads with traceback messages under a heavy load when a configuration change is made. There is no workaround.

- CSCdt01934

    The **clear host** [***** | *host name*] EXEC command may remove host names that have been statically configured. Only host names that have been learned dynamically should be removed. There is no workaround.

- CSCdt17100

    When the Multiple Resource Record feature is enabled (**ip director host** *host-name* **multiple** *integer*), the DistributedDirector may get into a CPU HOG mode. This may cause the watchdog timer to expire and the DistributedDirector to reboot. There is no workaround.

- CSCdt34919

    A Cisco 4500 series router may reload when using the c4500-w3-mz image. There is no workaround.

- CSCdt45871

    If one server goes down then comes back up when load balancing between three servers, that server will receive excessive traffic until its numbers are equal to the other two servers. Load balancing would then continue. This condition has been observed on a Cisco router that is running Cisco IOS Release 11.1(28)IA. There is no workaround.

- CSCdt48037

    When Border Gateway Protocol (BGP) sessions are reset with the **bgp log-neighbor-changes** router configuration command, "NOTIFICATION" messages that are sent or received are visible only if you enable the **debug ip bgp** EXEC command.

    Workaround: Upgrade to Cisco IOS Release 11.1(28)IA1.

Release 11.1(28)IA Caveats

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(28)IA. For additional caveats applicable to Release 11.1(28)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(27)IA Caveats/Release 11.1(28)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(27)IA. For additional caveats applicable to Release 11.1(27)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(26)IA Caveats/Release 11.1(27)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(26)IA. Unless otherwise noted, these caveats apply to all 11.1 releases up to and including 11.1(26)IA. For additional caveats applicable to Release 11.1(26)IA, see the caveats sections for newer 11.1 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 11.1(27)IA.

- CSCdm75198

    The DistributedDirector cache implementation results in losing memory, which will eventually cause the system to reload.

    A workaround is to disable DistributedDirector caching by using the **no ip director cache** command.

- CSCdp18279

    Using the **no ip director server** *ip-address* or **no ip director server** *ip-address* **connect** commands, which removes the remote server from the list of servers receiving regular verification connections, will sometimes cause the system to reload.

- CSCdp22168

    The DRP agent will incorrectly be reported as being down if the DistributedDirector receives some—but not all—of the DRP responses.

Release 11.1(25)IA Caveats/Release 11.1(26)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(25)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(25)IA.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(26)IA.

- CSCdm35542

    Portion metrics are not reset when servers are added. If you are using portion metrics for selecting a best server, and a server is added (or re-added because of previous unavailability), the internal portion tracking counts are not reset. This causes the new server to become the only selection until the portion counters reconcile.

Release 11.1(24)IA Caveats/Release 11.1(25)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(24)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(24)IA.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(25)IA.

- CSCdk09082

  Some types of incorrectly formed DNS packets may cause the system to reload.

- CSCdm05650

  DNS responses containing multiple PTR records (multiple names for the same IP address) may cause a reload.

Release 11.1(23)IA Caveats/Release 11.1(24)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(23)IA. For additional caveats applicable to Release 11.1(23)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(22)IA Caveats/Release 11.1(23)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(22)IA. For additional caveats applicable to Release 11.1(22)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(21)IA Caveats/Release 11.1(22)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(21)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(21)IA.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(22)IA.

- CSCdk32370

  In some situations, WebRedirector can gradually lose memory, which eventually forces a reload. This problem only occurs with WebRedirector and not with the DNS version of DistributedDirector. There is no workaround.

Release 11.1(20)IA Caveats/Release 11.1(21)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(20)IA. For additional caveats applicable to Release 11.1(20)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(19)IA Caveats/Release 11.1(20)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(19)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(19)IA.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(20)IA.

- CSCdk07961

    On devices running Cisco IOS Release 11.1(18) and earlier 11.1 versions, DNS queries originating from the router are at times sent on ports lower than 1024, which is usually considered the "privileged boundary" in many systems. Sending DNS queries on such ports can create problems with defining access lists for return UDP packets.

- CSCdk10968

    The DistributedDirector sometimes rejects DNS packets arriving from servers that use DNSSEC. Turning on the **debug domain** command shows the cause of the rejection as "Reserved bits are non-zero in DNS query."

- CSCdk13743

    In some situations, the DistributedDirector may incorrectly select the "best" remote server. In particular, if there is a tie among servers early in the list, and yet there is no tie when comparing them with the last server in the list, the DistributedDirector will not break the earlier tie at the next priority level. Instead, it will take the current "best" selection as being the ultimate "best." There is no workaround.

- CSCdk15000

    In situations where a "best" server selection is made at a particular priority level after a previous tie for "best," an incorrect selection of "best" server may be made. Also, servers found to be "down" and servers with administrative preference of "0" are not correctly "deselected."

- CSCdk19537

    If more than one priority level is configured and if all server metrics at the highest priority level are "incomplete," the selection algorithm will select the first server instead of proceeding to the next highest priority level.

- CSCdk20154

    In cases where two servers are tied for "best" and two other servers appearing before them in the list were previously tied for "best," one or more of the first set of servers is not correctly removed from selection when the new "best" server is established.

Release 11.1(18)IA Caveats/Release 11.1(19)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(18)IA. For additional caveats applicable to Release 11.1(18)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(17)IA Caveats/Release 11.1(18)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(17)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(17)IA. For additional caveats applicable to 11.1(17)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(18)IA.

- CSCdj72252

  Under some rare circumstances when operating in Redirector mode for several days or weeks, the DistributedDirector may stop accepting connection requests. Normal operation will resume after you reload the DistributedDirector.

- CSCdj85430

  When DistributedDirector is configured so that a DRP server agent (router) is associated with more than one server, queries are not answered for 4 seconds or more. The workaround is to configure secondary IP addresses on the DRP server agent (router), one for each associated server. In interface configuration mode, use the **ip address** *ip-address ip-subnet-mask secondary* command to add a secondary address for each associated server.

Release 11.1(16)IA Caveats/Release 11.1(17)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(16)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(16)IA. For additional caveats applicable to 11.1(16)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(17)IA.

- CSCdj71008

  When using DRP metrics and two sort requests from the same client (IP address) arrive close together, the DistributedDirector only stores and sorts on the first DRP response; the second (or later) one is ignored. Because the DRP metric values are not stored, the server associated with the second DRP agent is never selected even if its metrics are better.

- CSCdj73354

  The **ip director host** *name* **connect** and **ip director server** *address* **preference** commands do not allow specification of per-service information. TCP connection status should be kept on a per-service basis. New commands are needed to configure per-service information and to associate the correct per-service information (status and administrative preferences) with the virtual host name being requested.

Release 11.1(15)IA Caveats/Release 11.1(16)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(15)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(15)IA. For additional caveats applicable to 11.1(15)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(16)IA.

- CSCdj61911

  When the DistributedDirector is sent a PTR DNS request for a host whose host name is longer than the `in-addr.arpa` record in the request, the request will corrupt memory resulting in a crash.

Release 11.1(14)IA Caveats/Release 11.1(15)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(14)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(14)IA. For additional caveats applicable to 11.1(14)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(15)IA.

- CSCdj43545

  If the **drp-external** metric is configured for a host, then the DistributedDirector does not update the **drp-external** and **drp-internal** values even though the DRP response containing values for these metrics is received correctly.

Release 11.1(13)IA Caveats/Release 11.1(14)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(13)IA. For additional caveats applicable to Release 11.1(13)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(12)IA Caveats/Release 11.1(13)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(12)IA. For additional caveats applicable to Release 11.1(12)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(11)IA Caveats/Release 11.1(12)IA Modifications

There are no known and documented serious defects unique to the Cisco DistributedDirector System Software for Cisco IOS Release 11.1(11)IA. For additional caveats applicable to Release 11.1(11)IA, access Cisco Connection Online (CCO) as described in the section "Cisco Connection Online" later in this document.

There were no major modifications made in this release.

Release 11.1(10)IA Caveats/Release 11.1(11)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(10)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(10)IA. For additional caveats applicable to 11.1(10)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(11)IA.

- CSCdj08596

    If multiple remote servers are configured, along with server status checking, via the **ip director host** *name* **connect** command, and if one or more of the remote servers are found to be in a down state, it is possible for the DistributedDirector to erroneously select a down server as the "best" server.

Release 11.1(9)IA Caveats/Release 11.1(10)IA Modifications

This section describes possibly unexpected behavior by Release 11.1(9)IA. Unless otherwise noted, these caveats apply to all 11.1 IA releases up to and including 11.1(9)IA. For additional caveats applicable to 11.1(9)IA, see the caveats sections for newer releases that precede this section.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, use the Documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All caveats listed in this section are resolved in Release 11.1(10)IA.

- CSCdj00643

    If multiple priority levels are configured for a host and are called upon in the sorting process, the DistributedDirector will possibly make an incorrect selection of the "best" remote server in some cases.

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.