



Release Note for the Cisco 11000 Series Content Services Switch

April 15, 2003



Note

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

Contents

This release note applies to software version 5.00 build 63 (b63), maintenance release for version 5.00, for the CSS 11050, CSS 11100, CSS 11150, and CSS 11800 content services switches. For information on version 5.00 commands and features, refer to the CSS 5.00 documentation located in http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/css_500/index.htm.



Note

Do not attempt to load, unpack, or configure a version 5.10 software image (for a Cisco CSS series 11500) on a Cisco 11000 series CSS.

This release note contains the following sections:

- [New Features in Software Version 5.00](#)
- [CSS Standard and Enhanced Feature Sets](#)
- [Before Upgrading the CSS Software](#)
- [Updating Management Information Base Files \(MIBs\)](#)
- [Operating Considerations](#)
- [CSS 11150 and CSS 11050 Units Shipped with Incorrect MAC Addresses](#)
- [Caveats](#)
- [Resolved Caveats](#)
- [Version 5.00 b63 Command Changes](#)
- [Version 5.00 b45 Command Changes](#)



Corporate Headquarters:

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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

- [Configuring kal-ap by VIP](#)
- [Korean Certification Information](#)
- [Cisco 11000 Series CSS Documentation Roadmap](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

New Features in Software Version 5.00

The following new features are supported in software version 5.00:

- Configurable Spanning Packets for HTTP Header Termination
- ArrowPoint Cookie Enhancements
- Configurable Flow Cleanup
- Zeroing Service Statistics Counters
- Enhanced SSL Load Balancing
- Client Side Accelerator
- Content Routing Agent (Boomerang)
- RADIUS Client
- VIP and Interface Redundancy Config Sync
- SNTP Client
- 64-Character DNS A-Record
- 255 Scripted Keepalives
- Content Requests Spanning Packets
- Device Management Over Secure Sockets Layer (SSL)
- Restricting SSH
- Enhanced Flow Resource Collection Functionality
- KAL-AP by VIP

For information on the commands added in version 5.00 b63, see [“Version 5.00 b63 Command Changes”](#) later in this chapter. For information on the commands added in versions 5.00 b45, see [“Version 5.00 b45 Command Changes”](#) later in this chapter.

CSS Standard and Enhanced Feature Sets

The CSS software is available in a Standard or Enhanced feature set. The Enhanced feature set contains all of the Standard feature set and also includes Network Address Translation (NAT) Peering, Domain Name Service (DNS), Demand-Based Content Replication (Dynamic Hot Content Overflow), Content Staging and Replication, and Network Proximity DNS. Proximity Database and SSH are optional features. If you are upgrading from the Standard to the Enhanced feature set or want to activate a CSS software option (for example, SSH Server) that you purchased, refer to the *Cisco Content Services Switch Getting Started Guide* for information on entering a license key.

Access to the Standard and Enhanced feature sets or Proximity Database require that you enter a software license key when you boot the CSS for the first time. If you enter the Proximity Database license key after booting the CSS, you must reboot the CSS before you can configure the Proximity Database so the CSS can re-allocate memory. For details, refer to the *Cisco Content Services Switch Getting Started Guide*.

If you configure your CSS for Proximity Database, you cannot use the CSS for load balancing. For details on configuring a Proximity Database, refer to *Cisco Content Services Switch Advanced Configuration Guide*.

Before Upgrading the CSS Software

Read the following information before you upgrade the CSS.

- If **rmon-history data-source** commands exist in your current startup-config file, you will receive startup errors when you upgrade the CSS to 5.00 build 63. In version 5.00, the ifIndex identifier is assigned differently from the way it was assigned in prior software versions. After you upgrade the CSS to 5.00 build 63, you must reenter *all* **rmon-history data-source** commands contained in your startup-config file.
- If you are upgrading from 3.xx to 5.xx and have a 3.xx Enhanced software license key, you must enter a 5.xx Enhanced license key during the CSS upgrade to 5.xx or you will receive startup errors when you attempt to enter Enhanced CLI commands. If you upgrade the CSS and do not enter a 5.xx Enhanced license key prior to upgrading to 5.xx:
 - a. Use the **license** command to change the license key.
 - b. Reboot the CSS without saving the running-configuration.
- If you are running SSH on a 3.xx CSS and you have disabled Telnet, you must enable Telnet prior to upgrading the CSS to 5.00 build 63. After you upgrade the CSS to 5.00 build 63, use the **license** command to enter the SSH license key.

Updating Management Information Base Files (MIBs)

Cisco recommends that you update the CSS MIBs after you upgrade the CSS software. CSS MIBs are included in the CSS GZIP file. During the software upgrade, the MIBs are loaded into the CSS /mibs directory.

To update the CSS MIBs on your management station after you upgrade the CSS:

1. FTP the MIBs from the CSS MIBs (/v1 or /v2) directory to your management station.
2. Load the MIBs into the management application.

Operating Considerations

The following operating considerations apply to the CSS 11050, CSS 11100, CSS 11150, and CSS 11800:

- The CSS does not NAT fragmented IP packets.
- The CSS content routing agent is compatible only with the Cisco Content Router 4430-B software version 1.1.
- If you are running the Inktomi® Traffic Server™ on a system that does not listen in promiscuous mode and you want to bypass the Inktomi Adaptive Redirect Module (that is, send traffic directly to port 8080 instead of port 80), specify the CSS service type as **type proxy-cache**. Configuring the CSS service type to **type proxy-cache** causes the CSS to perform full Network Address Translation (NAT) when directing traffic to the Traffic Server.
- When Cisco makes syntax changes to existing CLI commands, the CSS updates your startup-config automatically with most command syntax changes. For example, the CSS automatically updates the **web-mgmt state enabled** command in the startup-config to the new **no restrict web-mgmt** command.

If the CSS does not update a command syntax change in a startup-config automatically, a startup error is displayed. See the sections [“Before Upgrading the CSS Software”](#) and [“Caveats”](#) for information on which command syntax changes display startup-config errors.

- The War-FTP daemon is not supported for network-booting the system software.
- The Gigabit Ethernet module port statistics are an aggregation of all ports on the module.
- When using the domain hash load-balancing method with proxy cache services, you may see duplicate sites across caches because the CSS balances on the first GET request in a persistent connection unless the subsequent GET request does not match a rule with the same proxy service specified. If you are concerned with duplicate hits across caches, reset persistence to remap and disable persistence on the rule. Enter the **(config) persistence reset remap** command globally and the **(config-owner-content) no persistent** command on the content rule.
- You cannot have an SFM and an SFM2 in the same CSS 11800 chassis.
- Content replication does not support the WSFTP FTP application.
- When using the content **add dns** command, you must add DNS names in lowercase only. If you enter DNS names with a combination of uppercase and lowercase characters, a startup error appears and you must reenter the names in lowercase characters.
- You cannot add redundancy uplink services to content rules.
- A redundant VIP configuration can consist of only two CSSs.
- The *ethernet-n* format for specifying an interface-port in a CSS 11050 or CSS 11150 (for example, ethernet-2) is supported for software releases prior to version 5.00 to ensure backwards-compatibility with CSS startup configurations and scripts.
- In software versions prior to 5.00, the CSS 11800 Fast Ethernet Module and Gigabit Ethernet Module Link LEDs are on solid during bootup. In 5.00, the Fast Ethernet Module Link LEDs blink rapidly and the Gigabit Ethernet Module Link LEDs are off during bootup.
- When you configure a service as a subscriber, you must specify the access type for each subscriber using the **access ftp** command.
- In a network boot configuration, the config-path and the base directory path in the ftp-record associated with the network boot must not contain a pathname that conflicts with a non-network drive name (for example, c: or host:).

- The CSS may reclaim:
 - TCP flows that have not received an ACK or content request after approximately 15 seconds
 - UDP flows that have not received an ACK or content request after approximately 16 seconds

To prevent the CSS from reclaiming TCP or UDP flows to a specific source or destination port, use the **flow permanent** command and specify the TCP or UDP port number you do not want reclaimed.
- This operating consideration applies when connecting a Cisco Catalyst switch to a CSS using 802.1q and the spanning tree protocol. Cisco switches run a spanning tree instance per VLAN. When you configure an 802.1q trunk on an Ethernet interface, the Bridge Protocol Data Units (BPDUs) are tagged with the corresponding VLAN ID, and the destination MAC address 01-00-0c-cc-cc-cd is used. This allows Cisco switches operating in a non-Cisco (a mix of other vendors) 802.1q environment to maintain spanning tree states for all VLANs.

Though the CSS maintains a spanning tree instance per VLAN as well, it continues to use the standard 01-80-C2-00-00-00 destination MAC address for all BPDUs (tagged or untagged). When you connect a Cisco Catalyst switch to a CSS over an 802.1q trunk, the result is that neither switch will recognize the other's BPDUs, and both will assume root status. If a spanning tree loop is detected, the Catalyst switch goes into blocking mode on one of its looped ports.
- You cannot configure services learned through APP (that is, remote services) as preferred services in ACL clauses. A remote service learned via APP is of the form `ap-redirect@192.168.12.7` and can be seen on the **show service summary** screen. When you configure an ACL clause, you cannot use this service as a preferred service. If you save this clause in the startup-config and reboot the CSS, a startup error occurs because this service has not been learned through APP at this point. For example:


```
clause 10 permit any any destination any prefer ap-redirect@192.168.12.7
```
- When you configure Firewall load balancing, the VIPs must be configured on the CSS that is not on the Internet side of the firewalls. Do not configure content rules with VIPs on the CSS connected to the Internet side of the firewalls unless the servers are directly connected to the CSS.
- The CSS FTP server supports only active FTP. It does not support passive FTP.
- The CSS does not support a traceroute of a redundant IP interface.
- A subscriber's state will not be ready or will be in access failure until the publisher's state is ready.
- The CSS does not support VIP redundancy and box-to-box redundancy simultaneously.
- The CSS recognizes and forwards the following HTTP methods directly to the destination server in a transparent caching environment. However, the CSS does not load balance these methods.
 - RFC-2068: OPTIONS, TRACE
 - RFC-2518: PROPFIND, PROPPATCH, MKCOL, MOVE, LOCK, UNLOCK, COPY, DELETE
- Network boot is not supported on UNIX workstations.
- If the upgrade script fails while upgrading the CSS to the *same* version of software that is currently running, the CSS software directory will be incomplete. To reinstall the software, you must upgrade the CSS manually (that is, FTP the .adi to the CSS and perform a manual unpack).
- The CSS does not set up flows if the source or destination port is designated as port 67, 68, 137, 138, 161, 162, 520, or 8089 (UDP only).
- With software version 5.00.045 and higher, flow reclamation is always active. If you find that the CSS reclaims flows too quickly, enter the **flow long-lived** command in Global configuration mode to delay flow reclamation on a lightly loaded CSS. This command allows long-lived flows to continue even with a large period of inactivity. For command details, see [“Version 5.00 b45 Command Changes”](#) later in this document.

You can monitor connection resources with the **flow statistics** command. The Number of Allocated Flows field shows the total number of connection resources allocated and managed by this processor in multiprocessor platforms. The Number of Free Flows field shows the maximum number of connection resources available on this processor in multiprocessor platforms. This number is based on how much RAM is available after the software image and configuration load.

- When using Arrowpoint cookies, the CSS may experience performance delays. To improve the CSS performance, enter the **arrowpoint-cookie advanced** command in owner-content mode. This command improves CSS performance by mapping the Arrowpoint cookie flows in the fastpath (hardware). For command details, see “[Version 5.00 b45 Command Changes](#)” later in this document.

The following operating considerations and caveats apply to the CSS Device Management software.

- Use Access Control Lists (ACLs) to restrict device management access to specific IP address and subnets. Note that ACLs do not affect the Ethernet Management port.
- Always exit the browser after each device management session to clear the cache.
- You must enable JavaScript in your browser for the Device Management software to work.
- Navigation tree icons do not always display. The pages function correctly. Open a page by clicking on the corresponding text.
- Device Management supports the following browsers:
 - Microsoft Internet Explorer version greater than 4.0
 - Netscape Communicator 4.51 and 4.71
 - Netscape Navigator 4.08
- If your Web browser has a bookmark to the Device Management software (software version 4.10 or earlier) that includes a colon (:) and TCP 8081 management port number at the end of the IP address, the software redirects the address to the correct URL. If your Web browser does not have a bookmark to the Device Management software, be sure to include an ‘s’ in http:// in addition to the CSS IP address. For example: https://192.168.3.6.

CSS 11150 and CSS 11050 Units Shipped with Incorrect MAC Addresses

Cisco CSS 11050 and CSS 11150 units shipped from Cisco Systems between 09/27/01 and 05/30/02 may have an incorrect MAC address assigned to the device (defect CSCdy36787). The MAC address of those units is not owned by Cisco Systems or any other vendor. The MAC address of each unit, although not a proper vendor code, is still a unique address and does not cause operational issues for either the CSS 11050 or CSS 11150.

For those CSS units shipped between 09/27/01 and 05/30/02, the chassis may have an assigned MAC address in the range of aa-3b-b2-ce-70-00 to aa-3c-f5-cd-f0-15. To verify the MAC address of your CSS chassis, use the **show chassis** command to display the base MAC address for the CSS.

The CSS software has been modified to correct the MAC address issue. A table is built into the CSS to reprogram the MAC address to an appropriate address. The software containing the MAC address fix is included in the latest maintenance releases. It is available in WebNS versions 4.01.032x, 5.00.045x, and 5.00.063, available at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/webns-maint>

In order to change the base MAC address of your CSS, upgrade to the appropriate version. The MAC address modification occurs during the software upgrade.

A Level 4 log message indicates that the MAC address is successfully updated with the value of the new MAC address. On subsequent reboots, the defective MAC address is not found in the Chassis Module Id EEPROM and the update does not occur.



The MAC address change for your CSS is permanent regardless of the CSS software version that you upgrade or downgrade to after you load one of the CSS *x* versions stated above or CSS version 5.00.063 (or greater).

Caveats

The following caveats apply to software version 5.00 build 63:

- **CSCdw15723** - If you are running software version 5.0 and using the Proximity Database (PDB), do not introduce a CSS running software version 5.02 into the proximity mesh. Updates from a version 5.0 Proximity Database to a version 5.02 Proximity Database can cause the CSS to reboot.
- **CSCdw31969** - SNMP service transition messages may cause the SNMP trap queue to overflow.
- **CSCdu34502** - Do not use the Cisco Content Router 4430-B **bloat** and **fragment-size** options with the CSS content routing agent. Entering these options causes unexpected results.
- **CSCdv52072** - Removing a URL suspends the associated content rule. In software version 4.01, you would receive an error message.
- **CSCdy52161** - The CSS may become stuck in a loop when you attempt to use a MIB walker to examine the CSS SNMP tree and you reach the apCnsvcOwnName MIB object identifier. This issue typically occurs in a configuration where you have automatic services learned through an Application Peering Protocol (APP) session in a global server load-balancing (GSLB) environment. Workaround: Perform individual GETs of the CSS MIB objects you want rather than using a MIB walker.

Resolved Caveats

The following caveats have been resolved in software version 5.00 build 63:

- **CSCdx41911** - The CSS perform a system reboot if an HTTPS POST request is sent to the Device Management interface of the CSS. This may occur even if the sender of the request is not yet authenticated to the device. Further details are described in the advisory at: <http://www.cisco.com/warp/customer/707/css-http-post-pub.shtml>.
- **CSCdx00117** - If you configure the **flow-reset-reject** command on a content rule, the CSS may continuously send a TCP RST to all existing connections in response to retransmissions. After a flow has been deleted, and the accounting report sent, the CSS now clears the flag to send the reset.
- **CSCdy00253** - A problem has been resolved with Proximity, where you may be unable to correctly set the N3 size percentage from the CLI.
- **CSCdy00254** - When the CSS is configured to respond to DNS queries, the response does not have the Authoritative bit set. The Authoritative bit in the DNS response sent by the CSS, when acting as an authoritative DNS server, may be random.
- **CSCdx01430** - If you configure RADIUS on a CSS, the CSS incorrectly displays a startup-error for the RADIUS primary or secondary server, even though the server is configured properly.
- **CSCdx01565** - The CSS 11800 contains an internal communication network which is used to communicate between the various modules in the chassis. A “to-do” list of communication operations to be performed over this network is maintained in software (the netJobRing). Under certain conditions, if the netJobRing becomes full, this could potentially result in a console failure, keepalives not responding, and so on. You must reboot the CSS 11800 to bring them back up.
- **CSCdy02590** - Improve the **dnsflow enable** and **dnsflow disable** command hints to be more clear and concise.

- **CSCdx02753** - With a Layer 5 content rule configured, there could be instances when the CSS receives multiple instances of a SYN segment coming in for a flow that is already mapped to the CSS. The TCP/IP 3-tuple information (network number, subnet number, and host number) and the sequence number are the same as the SYN for the mapped flow, so the CSS forwards the SYN and the subsequent POST to the wrong server.
- **CSCdw05273** - With a domain record set up on the CSS, when the CSS sends a kal-ap request to another CSS for a domain name load value, the requesting CSS adds approximately 1 KB of zeros to the keepalive request. Kal-ap sends all of the data rather than sending only what is in the datagram. This is the case for both clear text and MD5 encryption. This padding causes every packet to be approximately 1108 bytes (standard) or 1112 bytes (encrypted) regardless of the actual request payload.
- **CSCdy06124** - When the CSS learns a service over an APP session and the length of the service name (including the appended IP address of the CSS owning this service) is exactly 32 characters, the CSS may perform a system reboot. A name and IP address with a combined length of 32 characters exceeds the 31 character limit on the service name. Workaround: Since the length of IP addresses can be variable, a reasonable workaround for this issue is to keep the service names short (fifteen characters or less) so that when appended with any IP address, the total length of the service name does not exceed 31 characters.
- **CSCdy06152** - If the **application ssl** command appears before the **port** command in a content rule, during the next reboot the CSS generates startup errors. The **application ssl** and **port** command checks are now performed when you activate the content rule to prevent the startup-error problem.
- **CSCdx07187** - The CSS performs an unexpected system reload when OSPF submits a default route with a non-null mask. The CSS now ignores the faulty submission.
- **CSCdy07367** - Adds two new syslog message when you reboot the CSS from the CLI (`Reboot` command entered via CLI and `Shutdown` command entered via CLI).
- **CSCdx08287** - With very large content replication configurations, it is possible for a deadlock to occur during the initial replication.
- **CSCdx08332** - If you delete a non-OSPF route and the CSS receives a new OSPF route to a destination, the CSS does not update the SFP routing table.
- **CSCdx13029** - In some networks, the CSS withdraws firewall routes before the firewalls complete a redundancy transition. This causes unnecessary disruption in the network because the routes are available almost immediately after the withdrawal when the firewalls recover. The **ip firewall timeout** command has been added to allow you to configure the CSS to avoid these unnecessary route changes. For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.
- **CSCdx13320** - If you configure a static route to take precedence over a RIP route, the CSS does not update the **show ip route** command output right away. The new static route should appear even while the old RIP route is waiting to be removed from the route table.
- **CSCdx13475** - Some spare tasks within the CSS do not properly clean up their file descriptor resources upon completion. If the CSS reaches the point where all file descriptors are in use, the console or Telnet session may become unresponsive.
- **CSCdy13359** - The number of configurable permanent ports supported with the flow permanent command is increased from 10 to 20 (**flow permanent port11** *portnumber* to **flow permanent port20** *portnumber*). For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.

- **CSCdx14704** - If a content rule has all services of **type redirect** and the load balancing algorithm is **balance weightedrr** (weighted roundrobin), load balancing is not performed using weighted roundrobin, but instead uses roundrobin as the balancing mechanism. Previously, the only load balancing method that worked on a content rule with only redirect services was roundrobin. Added the ability to use **balance weightedrr** on this type of content rule as well.
- **CSCdy16014** - In some instances, APP can cause a software assertion under very large content rule sharing configurations at undefined timing intervals.
- **CSCdy16570** - In some cases, the CSS may become unresponsive and perform a system reboot because it ran out of file descriptors due to a leak in the APP shutdown code path.
- **CSCdu16696** - The Device Management software only supports 128-bit encryption. Browsers that support less than 128-bit encryption will not work with the CSS Device Management and will generate a message informing you of this limitation.
- **CSCdx18636, CSCdx39369, CSCdu46997** - Resolved a number of issues with the Current Connection counter in the **show service** output, such as:
 - The wrong service did not decrement at flow teardown time because the internal WCC in/out cookies contained different service indexes.
 - With a persistent connection, it was possible to overwrite the internal WCC in cookie server and lose track of which service index needs to be decremented at flow teardown time.
 - When a service goes down, this sometimes cleared the Total Connections counter in the **show service** output.
- **CSCdx18725** - When using box-to-box redundancy with services configured with HTTP keepalives, the internal hash value (or checksum) of the keepalive URI should be zeroed when the CSSs change mastership, unless the keepalive hash value was specifically configured. Dynamically changing pages could cause keepalives to not come up unless this is done.
- **CSCdx18853** - When using the **advanced-balance wap-msisdn** command, the CSS 11800 sometimes does not properly distribute the flows because the sticky table does not update across all SFPs. In addition, the CSS does not update the sticky counters properly for the **advanced-balance wap-msisdn** sticky type.
- **CSCdy21290** - A Layer 4 content rule with a load balancing method that promotes the content rule to Layer 5 (for example, **balance urlhash**) can result in the transmission of a TCP RST back to the client when the CSS makes a request using a HTTP CONNECT method.
- **CSCdy21617** - Clients may remain stuck to a primary sorry server even when local services resume operation. For example, if a CSS has either a Layer 3 or Layer 4 content rule with **advanced-balance sticky-srcip** or **advanced-balance sticky-srcip-destport** and a primary or secondary sorry server. The CSS then becomes inactive. Once a client is stuck to the sorry server, all new requests remain stuck to the sorry server even after the local service is back up.
- **CSCdx25872** - If you configure a Layer 5 content rule without a VIP on a CSS and open a Webmail session across a TCP connection, the CSS resets the TCP connection. Workaround: Remove the Layer 5 rule and configure a Layer 4 rule.
- **CSCdy26205** - When you specify a SNTP, OSPF, or RIP command, the CSS may perform a system reload.

- **CSCdy26277 & CSCdy27760** - Resolved a number of issues with the **script play commit_vip_redundancy** command, such as:
 - Option **-s** does not function properly
 - Configuring two circuits for VRID to function
 - Inconsistent operation of running a script with the **-a** option
 - Problems synchronizing the configuration if a VLAN has been deconfigured
- **CSCdx27019** - RADIUS access-request packets sent by a CSS have empty fields for attribute 4 (NAS-IP-Address) and attribute 61 (NAS-Port-type). This issue can cause interoperability problems with some RADIUS server features that are based on those two attributes (for example, the Cisco ACS Network Access Restriction feature). To address this problem, the CSS now supports the **radius-server source-interface ip_or_host** command, where you specify the IP address or host name of the CSS, which is either a CSS circuit or Ethernet management port address. Certain RADIUS servers require that the **radius-server source-interface ip_or_host** be configured to accept authentication from the CSS as a RADIUS client. Note that this IP address is used for the NAS-IP-Address RADIUS attribute in the RADIUS Authentication Request. For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.
- **CSCdy27434** - The CSS now responds to kal-ap-vip queries. The kal-ap-vip query packets contain VIP addresses, and the CSS matches the VIP addresses with configured content rules to return status and load. For command details, see the “[Version 5.00 b63 Command Changes](#)” and “[Configuring kal-ap by VIP](#)” sections later in this document.
- **CSCdy27476** - The **dns-record** command has been enhanced to support the **kal-ap-vip** keepalive option. When you specify this option, the CSS generates kal-ap-vip queries for monitoring status and load. For command details, see the “[Version 5.00 b63 Command Changes](#)” and “[Configuring kal-ap by VIP](#)” sections later in this document.
- **CSCdw27861** - When you configure a DNS record for a keepalive of type **kal-ap**, the CSS incorrectly report loads for VIP redundancy. If you configure a domain name on a content rule using the **add dns domain_name** command and the VIP for the rule is currently in backup mode (because of VIP redundancy) the CSS reports a load for the services configured on that content rule. Because the content rule is suspended by VIP redundancy, the CSS should report a load value of 255 to indicate a failure.
- **CSCdy31645** - Rejected SNTP packets are logged for IPv4 and SNTP subsystems at the **notice-5** level, which is below the **default-4** level and can often be overlooked. All rejected SNTP packets are now logged at the **warning-4** level rather than **notice-5** level.
- **CSCdx32956** - A RADIUS authentication request may be overwritten if two users log in simultaneously. This RADIUS authentication issue can also occur if the primary server is probed and the secondary server is used for authentication.
- **CSCdx35296** - The **show radius config all** command may not display the correct state of the primary RADIUS server. When the CSS probes a primary RADIUS server, the time to wait for a response must be less than the dead timer or the state of the primary server may be inconsistent with the **show radius** command output.
- **CSCdw36620** - Adds the **show version** command to be consistent with other CSS releases and Cisco Systems software products. The **show version** command is the equivalent of the existing **version** command. Both the **show version** command and the **version** command are supported. For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.

- **CSCdy36787** - Cisco CSS 11050 and CSS 11150 units shipped from Cisco Systems between 09/27/01 and 05/30/02 may have an incorrect MAC address assigned to the device. Those CSS 11050 and CSS 11150 units have a MAC address that begins with aa- (aa-3b-b2-ce-70-00 to aa-3c-f5-cd-f0-15). The MAC address is not owned by Cisco Systems or any other vendor. Note that the MAC address on each unit is still unique and the CSS will function normally. Refer to “[CSS 11150 and CSS 11050 Units Shipped with Incorrect MAC Addresses](#)” for details.
- **CSCdy21141** - The CSS does not clean up idle flows until one-eighth of the total number of flow control blocks (FCBs) are in use. In this way, a CSS that is lightly loaded does not tear down idle flows when those resources are not needed. This practice left more active FCBs on ports and made it appear that there are more active flows than actually exist. For this reason, flow resource cleanup is configurable through the **flow long-lived** command (defect CSCdx39590). The default behavior is that flow resource cleanup is always running. With CSCdy21141, the command now delays garbage collection until one-fourth of the total number of flow control blocks (FCBs) are in use. See the **flow long-lived** command in the “[Version 5.00 b45 Command Changes](#)” section.
- **CSCdw35822** - Using a one-armed router configuration and an SSL rule with a URL defined, the CSS could leak flow control blocks (FCBs).
- **CSCdt36894** - If you enter the **proximity clear** command, cancel it, and then reenter the command, the PDB may no longer respond to database lookup requests.
- **CSCdx39613** - When you configure the **dnsflow disable** command and an ACL is specified to direct traffic to a source group, the CSS may perform a system reload when the ACL clause is hit.
- **CSCdx40769** - When a redundant interface or VIP MAC address switches between a master CSS and a backup CSS a number of times in quick succession, the bridge entry may be freed too many times and cause an unexpected system reload.
- **CSCdw41583** - If the Device Management interface is active for an extended period of time, an unexpected system reload could occur because of a decrease of available memory.
- **CSCdx42545** - The CSS arrowpoint-cookie uses “Tues” instead of “Tue” in the day of week field (of the cookie expiration field) and uses capital letters for the month field of cookie expiration. The CSS now supports the **arrowpoint-cookie rfc2822-compliant** command. When enabled, this command causes the CSC arrowpoint-cookie expiration time syntax to be RFC2822 compliant by using only three character days of the week (for example, “Tue” rather than “Tues”) and capitalizing the first character of the month (for example, “Jan” rather than “JAN”). For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.
- **CSCdx45147, CSCdx59152** - Logging from the CSS to a syslog host does not work properly. The CSS does not check properly for the loghost facility level to determine whether a syslog message should be sent.
- **CSCdx45606** - If the CSS encounters an EPIF reset, the physical interface configuration may not be restored properly. When the EPIF bank comes back up, the speed and duplexity of the interface may be incorrect and the flow rate may be severely impacted. EPIFs are associated only with 10/100 Ethernet ports.
- **CSCdx46445** - Uniform Resource Locator Qualifier Lists (URQLs) do not work properly when configured with domain names. A workaround for this caveat is to define the domain name in the URQL with all uppercase letters. For example, if the domain you want is *www.test.com*, then define it as domain *WWW.TEST.COM* in the URQL.
- **CSCdx46512** - If you change the SSHD listen port on a CSS using XML or SNMP, the CSS may perform a system reload during bootstrap.
- **CSCdx46453** - There are overlapping ranges in static ARPs and source groups. If a source group address overlaps with a static ARP address, and you remove the static ARP entry, the CSS displays an error message about the conflict.

- **CSCdt49036** - The CSS supports a maximum of 15 active ECMP routes.
- **CSCdx49132** - With a Layer 5 domain content rule that includes a URL/port of the form “url /brandnewproducts:8001/*”, the CSS may not match on anything past the colon. The CSS now matches on the entire host tag including the port number. Normally, port 80 traffic does not use a port number in the domain name. To specify a port other than port 80, enter the domain name with the port number exactly. Separate the domain name and the port number with a colon. For example: (config-owner-content[arrowpoint-rule1])# url “//www.arrowpoint.com:8080/*”
- **CSCdu49859** - Adds the ability to configure the flow timeout value for up to 10 ports through the **flow port1 portnumber timeout value** to **flow port10 portnumber timeout value** commands. For command details, see “[Version 5.00 b63 Command Changes](#)” later in this document.
- **CSCdx50100** - The TFTP protocol may not work properly through a source group. The TFTP protocol listens on port 69. The reply packet from the TFTP server changes its UDP source port from port 69 to a higher UDP port number (per RFC 1350). The CSS 11000 source group incorrectly assumes that port 69 replies and disrupts the TFTP transfer. The CSS now checks that the port number has changed so that it does not get overwritten with the old TFTP port information.
- **CSCdx50286** - If a CSS receives the Telnet NOP (No Operation) command, a Telnet session to the CSS may become unresponsive.
- **CSCdx52724** - On a standalone CSS 11050 or CSS 11150, if Ethernet ports 5 through 8 have an EPIF reset the Gigabit ports on the CSS may become unusable.
- **CSCdv52379** - If a client sticks to a server based on the Secure Socket Layer (SSL) version 3 session ID and the server is disabled, the CSS incorrectly forwards a subsequent request to the disabled server from that SSL Session ID. If you make configuration changes to the disabled server (for example, specification of the maximum connections value), the CSS performs a system reload when it tries to forward the request to the disabled server.
- **CSCdx54742** - When using a Layer 5 content rule with a header-field group, the content rule does not match properly when the HTTP method is CONNECT.
- **CSCdx55312** - In a VIP redundancy configuration (active-backup), setting the interface to the 100-Mbps Ethernet port could cause physical link failures and affect VIP redundancy operation. Workaround: Use the **phy** command to configure the interface to either **auto-negotiate** or to **10-Mbits**.
- **CSCdx55560** - If the event count for a DoS attack is greater than 10 million, the **show dos** command may become unresponsive.
- **CSCdx56068** - Performance of the Device Management interface may be extremely slow when accessed through a HTTPS proxy, which can make the Device Management interface unusable. The issue is related to an SSL encryption key.
- **CSCdx56298** - The CSS ignores attempts to modify the subnet mask of a configured circuit IP address. To modify the subnet mask of a circuit IP address, you must first delete the IP address. The CSS now displays a warning message to notify the user.
- **CSCdx56706** - ACLs appear to be overridden by equal-cost multipath (ECMP) settings. If an ICMP packet (which is not destined to a local address) hits an ACL that has a preferred service configured on it, the CSS now routes the packet toward the preferred service address instead of using the ECMP setting (such as **ip ecmp address** or **ip ecmp roundrobin**).
- **CSCdw57754** - Under test conditions with excessive Telnet session connections and disconnections using a script, it is possible to cause the Telnet session, and sometimes the console, to become unresponsive.

- **CSCdx59034** - Duplicate MAC addresses on the same VLAN may cause memory fragmentation, which may eventually lead to the CSS performing a system reload and rebooting. The duplicate MAC addresses can cause the forwarding entry to continually be learned and updated by the CSS on different ports.
- **CSCdx59081** - If a CSS receives a UDP packet that hits a content rule, the CSS performs a system reload.
- **CSCdx60204** - Entering the **icp shell** command in debug mode may cause the CSS to perform an unexpected system reload. Do not use the **icp shell** command; it is not a supported command.
- **CSCdx62611** - If the CSS retransmits a SYN/ACK back to the client when spoofing the connection, the CSS does not include any TCP options. The CSS should include the options that the client transmitted in the initial TCP SYN.
- **CSCdx63118** - If a CSS performs an SNMP poll for the apIpv4RedundancyVIPState OID at the same instance when you delete the redundant VIP, the CSS may unexpectedly perform a system reload.
- **CSCdx65501** - With an **advanced balance arrowpoint-cookie** content rule containing one service, the CSS may try to perform a server remap to the same server if multiple GETs are received before the server has a chance to respond to the first GET. For example, when the CSS receives two GETs on a persistent TCP connection, and neither GET has the arrowpoint cookie, in some instances the first GET load balances to S1 and the second GET causes the CSS to perform a server remap to S1.
- **CSCdx69257** - The CSS shows inconsistent behavior with IP routing. The internal Ipv4 tree does not update properly.
- **CSCdx69313** - When using PASV FTP to a VMS server, the PASV FTP 227 response is not NATed properly by the CSS. The CSS looks for the "(" character as the delimiter for the IP address in a PASV FTP 227 response. RFC-1123 states that this character cannot be relied upon and the application "must scan the reply for the first digit of the host and port numbers". The CSS now scans the PASV FTP 227 response for the first digit of the IP address if the "(" character is not found.
- **CSCdx69997** - When using scripted keepalives, the CSS should internally adjust the keepalive frequency to be appropriate for the number of scripted keepalives configured on the CSS. With greater than 30 scripted keepalives, the CSS reverts to the default values.
- **CSCdx71712** - An HTTP keepalive stops transmitting over a period of time. The keepalive on a service then becomes stuck and the service keepalive goes down. This issue occurs because the keepalive "InProgressArray" for this service index becomes stuck in the TRUE state.
- **CSCdx74081** - When performing an SNMP NEXT of the apCntOwner MIB, the CSS may enter a NEXting loop if a content rule name contains more than 32 characters. This issue may occur when the CSS is using APP to learn content rules from another CSS and the prefix "AUTO_" is prepended to the content rule name. In this instance, the content rule name must be 26 characters or less to provide room for expansion.
- **CSCdx74811** - When you configure the CSS with a VIP and to NAT packets, the ICMP header of ICMP packets type 3 (destination unreachable) and code 3 (port unreachable) is incorrect, which can result in the receiving device dropping the ICMP packet and the connection timing out. If an ICMP Port/Destination Unreachable is received on a flow, the IP Header must be NATed as well as the embedded IP header within the ICMP data. If the length of the ICMP header plus the embedded IP header/data exceeds 36 bytes, the resulting ICMP checksum in the packet sent by the CSS is incorrect.
- **CSCdx75994** - A flow control block (FCB) leak occurs due to asymmetric routing in the network. In this case, the SYN/ACK that is returned from the server does not come in on the port anticipated by the routing table. This issue can be caused by a dual NIC configuration on the servers.

- **CSCdx76867** - An IP fragment packet, that is destined to a VIP, is routed back to the default route and looped between the gateway and the CSS until the time-to-live (TTL) expires. The IP fragment packets are not discarded, but instead routed to the default gateway, which causes a routing loop to occur between the CSS and the router.
- **CSCdx77068** - The CSS, after receiving a gratuitous ARP Response, fails to forward TCP packets to the new MAC address. The CSS understands the Gratuitous ARP Response, updates the ARP table accordingly, and forwards ICMP packets to the correct MAC address. However, the CSS keeps forwarding TCP packets to the old (incorrect) MAC address. This issue occurs only with flows to services which are not on a subnet shared by the CSS, and only when the gratuitous ARP is received without loss of connectivity to the next hop to the service. The resolution for this defect creates new flows using the correct next hop MAC address, but does not change the next hop MAC address of existing flows.
- **CSCdw78256** - If the **bridge** command options **max-age**, **forward-time**, and **hello-time** are in the CSS startup-config, the CSS does not properly apply the options upon reboot.
- **CSCdx84439** - The v2/dqlxext.mib has a typographical error. “apDQLdoaminGroup” should be “apDQLdomainGroup”.
- **CSCdx80284** - If a content rule with **advanced-balance arrowpoint-cookies** has no local services alive, and an HTTP request is made to the VIP, the CSS may perform a system reload.
- **CSCdv80661** - Configuring an interface on the CSS to a setting other than auto-negotiate (using the **phy** command) may result in a slower FTP connection on that interface.
- **CSCdx81573** - Using OSPF, if there were multiple route flaps, it may be possible for the IPV4 OSPF task to cause all IPV4 functions to cease.
- **CSCdw82060** - SSH vulnerabilities are checked only by inspecting the reported SSH version, which may leave an opportunity for false positives. When the CSS is scanned by the ISS scanner, two vulnerabilities are reported. The first vulnerability is described at <http://www.cert.org/advisories/CA-1998-03.html> and the second vulnerability is described at <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0144>. Note that the CSS is not vulnerable to the first issue. The CSS does not have the UNIX file system, and this vulnerability is not applicable to the CSS. The second vulnerability, described by CAN-2001-0144, has been resolved by CSCdx59197.
- **CSCdx83367** - A flow control block (FCB) leak may be caused by a Layer 5 content rule with multiple remaps in an equal cost multi path (ECMP) configuration. The SYN-mapped FCB may be lost if the content frame came in on a different port.
- **CSCdw84794** - When you enable and disable Telnet sessions to the CSS 11800 in a rapid succession, you may cause the SCM to become unresponsive and cease CSS management access.
- **CSCdx85356** - The RADIUS username and password maximum lengths are 16 bytes each, but TSM (Telnet, FTP, or SSH) allows you to type up to 32 characters for each. Entering a maximum of 32 characters can cause the CSS to perform a system reload.
- **CSCdx85579** - With a sorry server of service **type redirect**, the CSS may perform a system reload on a persistent connection when the second HTTP GET hits the sorry server.
- **CSCdv86041**, **CSCdw90381** - Using the **proximity assign** command to make a subnet less specific may cause a CSS to unexpectedly perform a system reload.
- **CSCdw87925** - Some APP sessions within the CSS do not properly clean up their file descriptor resources upon completion. If the CSS reaches the point where all file descriptors are in use, this may cause the console or Telnet session to become unresponsive.

- **CSCdx88928** - If the sticky database has no entries available due to a configured sticky inactivity timer on the content rule, the CSS may not efficiently forward new incoming SSL flows. The flow may be unmapped in the fastpath and all subsequent SSL frames may be forwarded in the slow path.
- **CSCdw90533** - When entering multiple **clear running-config** and **copy startup-config running-config** commands in a loop with a five second pause between each command, the following message appears: `IMM message not deliverable, message queue full.`
- **CSCdx91988** - If an HTTP request spans multiple packets, and the packets arrive at the CSS out of order, the CSS may make the wrong load-balancing decision.
- **CSCdx93247** - The CSS supports persistent HTTP 1.1 keepalives. The initial request for an HTTP keepalive or ICP probe uses HTTP 1.0 but it should be HTTP 1.1.
- **CSCdx94347** - When running box-to-box redundancy with the physical links set to 100 Mbits-FD, and the crossover cable is disconnected from one or both CSSs and then reconnected, both CSS devices remain in a Master state (the redundancy-protocol does not run). If one or both physical links are set to auto-negotiate, this problem does not occur.
- **CSCdx94309** - The CSS 11800 SCM may become unresponsive due to an IPV4 RTM semaphore deadlock issue.
- **CSCdx98818** - If you attempt to run the `commit_redundancy` script between a pair of CSS 11050s, the configuration synchronization script may fail in the verify state when VIPs are missing in some of the content rules on the backup device. In this specific case, the master CSS is configured for DNS server functionality and there is a conflict when the master CSS shares DNS information over the APP session (the VRRP link between the two CSSs). The APP session over the VRRP link included the `config-sync` and `rcmd` functions.

Version 5.00 b63 Command Changes

Table 1 and Table 2 list the commands and options that have been added to and changed in software version 5.00 b63.

Table 1 CLI Commands Added in 5.00 b63

Mode	Command and Syntax	Description
General Commands: SuperUser, User, and all modes	show ip firewall	Displays the configured values of the IP firewall keepalive timeout (see the ip firewall timeout number command below) and the state of each firewall path configured on the CSS.
	show version	Displays the network boot configuration. Note Use the version command in SuperUser mode to display the network boot configuration.
Global	arrowpoint-cookie rfc2822-compliant	Causes the arrowpoint-cookie expiration time syntax to be RFC2822 compliant by using only three-character days of the week and capitalizing the first character of the month. The default is disabled. For example: day: Mon, Tue, Wed, Thu, Fri, Sat, Sun month: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

Table 1 CLI Commands Added in 5.00 b63 (continued)

Mode	Command and Syntax	Description
Global	flow port1 <i>portnumber</i> timeout <i>value</i> to flow port10 <i>portnumber</i> timeout <i>value</i>	Configures the flow timeout value for up to 10 ports through the flow port1 <i>portnumber</i> timeout <i>value</i> to flow port10 <i>portnumber</i> timeout <i>value</i> commands. The timeout value is an integer from 1 to 600 seconds (10 minutes). Note that a configured flow permanent port takes precedence over a configured flow timeout value. If you do not configure a flow timeout value the default timeout takes effect, as follows: <ul style="list-style-type: none"> • Default TCP - 15 seconds • Default UDP - 16 seconds • NFS (port 2049), CHAT (port 5190), HTTP (port 80) - 8 seconds • FTPDATA (port 20), FTPCTRL (port 21), TELNET (port 23), SSHD (port 22), SOCKS (port 1080), FWGUI1(port 258), SQLSRV (port 156), ORACLE1 (port 1521), ORACLE2 (port 1526), and SMTP (port 25) - 600 seconds
	ip firewall timeout <i>number</i> no ip firewall timeout	Specifies the number of seconds the CSS waits to receive a keepalive message from the remote CSS before declaring the firewall to be unreachable. The two CSS switches at the endpoints of the firewall configuration must use the same firewall keepalive timeout value. Otherwise, routes on one CSS may not failover simultaneously with those on the other CSS. This could permit asymmetric routing to occur across the firewalls. The timeout range is 3 to 16 seconds. The default is 3 seconds. Note The amount of time required for a firewall path to become available is unaffected by this command, and remains at three seconds. To reset the firewall timeout to the default value of three seconds, use the no form of the command.
	radius-server source-interface <i>ip_or_host</i>	Specifies the IP interface where RADIUS packets are transmitted to and from the RADIUS server. Specify the IP address or host name of the CSS. The IP address or host name must match either a CSS circuit or Ethernet management port address. Enter an IP address in dotted-decimal notation or in host-name format. The default is 0.0.0.0. Certain RADIUS servers require that the radius-server source-interface <i>ip_or_host</i> be configured in order to accept authentication from the CSS as a RADIUS client. Note that this IP address is used for the NAS-IP-Address RADIUS attribute in the RADIUS Authentication Request.

Table 2 CLI Commands Changed in 5.00 b63

Mode	Command and Syntax	Change
Global	flow permanent port11 <i>portnumber</i> to flow permanent port20 <i>portnumber</i>	The number of configurable permanent ports supported with the flow permanent command has been increased from 10 to 20. Note Do not configure the flow permanent command without enabling the cmd-sched command to periodically remove the permanent port and allow for cleanup.
	dns-record alns <i>dns_name ip_address {ttl_value {single multiple {kal-ap kal-ap-vip kal-icmplkal-none {ip_address2}...}}</i>	Added the kal-ap-vip option to the dns-record command , which allows a CSS client to request load and status information about a VIP configured on multiple content rules from a CSS agent. For details, see “Configuring kal-ap by VIP” later in this document.

Version 5.00 b45 Command Changes

Table 3 lists the commands and options that have been added to software version 5.00 b45.

Table 3 CLI Commands Added in 5.00 b45

Mode	Command and Syntax	Description
General Commands: SuperUser, User, and all modes	zero service [total-connections total-reused-connections state-transitions]	Sets specified statistics counters to zero for all services on the CSS. <ul style="list-style-type: none"> The total-connections option sets the Total Connections counter to zero for all services. The total-reused-connections option sets the Total Reused Conns counter to zero for all services. The state-transitions option sets the State Transitions counter to zero for all services.
Global	flow long-lived no flow long-lived	Delays flow reclamation on lightly loaded CSSs to allow long-lived flows to continue even with a large period of inactivity. This command is disabled by default. Use this command only if the CSS reclaims flows too quickly and the number of flows on the CSS is relatively low. You may find this command particularly useful for a database application. To disable this command, use the no form.
	spanning-packets <i>packets</i> no spanning-packets	Allows you to configure the number of packets spanned for the search of the HTTP Header termination string. Enter a <i>packets</i> value from 1 to 20. The default is 6. The CSS will try to match a content rule even if the termination string does not appear within the number of spanned packets allowed. Previously, the CSS would send a reset (RST) if the termination string was not found within the number of spanned packets. To reset the number of packets spanned to the default value, use the no form of this command.

Table 3 CLI Commands Added in 5.00 b45 (continued)

Mode	Command and Syntax	Description
Global (continued)	ssl-l4-fallback disable enable	<p>Disables or reenables the CSS insertion of the Layer 4 hash value, based on the source IP address and destination address pair, into the sticky table. By default, the CSS inserts the Layer 4 hash value into the sticky table.</p> <p>Insertion of the Layer 4 hash value into the sticky table occurs when more than three frames are transmitted in either direction (client-to-server, server-to-client) or if SSL version 2 is in use on the network. If either condition exists, the CSS inserts the Layer 4 hash value into the sticky table, overriding the further use of the SSL version 3 session ID.</p> <ul style="list-style-type: none"> The disable option disables the CSS from inserting the Layer 4 hash value into the sticky table and continues to look for SSL version 3 session IDs. The enable option resets the CSS to its default behavior of inserting a Layer 4 hash value into the sticky table. <p>The ssl-l4-fallback command is only applicable when the (config-owner-content) advanced-balance ssl method is specified for a content rule, which forces the content rule to stick to a server based on SSL version 3 session ID.</p> <p>Do not enter the ssl-l4-fallback disable command if SSL version 2 is in use on the network.</p>
Owner-content	arrowpoint-cookie advanced no arrowpoint-cookie advanced	<p>The new advanced option improves performance with Arrowpoint cookies where large amounts of data (for example, graphics) are returned from the server by mapping the Arrowpoint cookie flows in the fastpath (hardware). Use this option only if you are experiencing performance delays with Arrowpoint cookies. This option is disabled by default.</p> <p>To disable this option, use the no form of this command.</p>
	zero {total-connections total-reused-connections state-transitions {service name}}	<p>The new total-connections, total-reused-connections, and state-transitions options for the zero command set the applicable counters to zero for a specified service or all services of the current content rule.</p> <p>When you use the service name option, only the counter for the specified service is set to zero.</p>

Configuring kal-ap by VIP

Kal-ap by VIP extends the functionality of kal-ap (the CSS keepalive by domain) by providing load and status responses to queries for virtual IP addresses (VIPs) configured on multiple content rules rather than for domains configured on a single content rule as provided with kal-ap. This feature allows greater flexibility and accuracy of load and status reports for multiple content rules that are configured with the same VIP. This feature also eliminates the need for configuring domain names on a CSS that is responding to kal-ap by VIP queries only and is not running a local DNS server.

Overview

In a manner similar to kal-ap, kal-ap by VIP has two main components:

- Client
- Agent

A client is a CSS that requests load and status information for a VIP from an agent. You configure a client to generate queries using the **dns-record** command. For details, see “[Configuring a kal-ap by VIP Client](#)” later in this section.

An agent is a CSS that responds to client queries with load and status reports for the requested VIPs. A kal-ap by VIP agent can handle and respond to queries from local or remote CSSs (including itself) and other supported devices. No additional configuration is required for the agent.

To best service requests for a domain when making GSLB decisions, a CSS may need to consider the keepalive status and load information of all content rules sharing the same VIP. Often, a kal-ap by VIP configuration has at least two content rules to handle domain traffic: one for port 80 (TCP) and one for port 443 (SSL). The load reported by the agent is the average load of all the content rules that share the same VIP, unless a content rule is suspended.

In order for a kal-ap by VIP agent to return a load value from 2 to 254 (indicating an Alive status) for a requested VIP, at least one service must be Up on each content rule sharing the requested VIP. For a requested VIP, if all services configured on one content rule are Down, or if one content rule is suspended, the agent reports a load of 255, indicating that the VIP is unavailable.

Configuration Requirements

Kal-ap by VIP requires that you configure the following:

- Application Peering Protocol-User Datagram Protocol (APP-UDP) - Used to transmit kal-ap by VIP datagrams. (For information on configuring APP-UDP, refer to the *Cisco Content Services Switch Advanced Configuration Guide*.) The datagrams can contain a mix of both kal-ap (by domain or tag) and kal-ap by VIP requests.
- **dns-record** command with the **kal-ap-vip** option - Used to configure a kal-ap by VIP client. See “[Configuring a kal-ap by VIP Client](#)” later in this section.



Note

You can configure **kal-ap-vip** and **kal-ap** on the same CSS. If you configure **kal-ap** on a CSS, you must also configure the **add dns** command with the appropriate domain names on the CSS acting as an agent. The agent will respond with the load information for a VIP and/or a domain, as appropriate. For information on the **add dns** command, refer to the *Cisco Content Services Switch Advanced Configuration Guide*.

Configuring a kal-ap by VIP Client

To configure a kal-ap by VIP client on a CSS to allow the CSS to query a kal-ap by VIP agent for keepalive information on multiple content rules, use the **kal-ap-vip** option of the **dns-record** command. The syntax for this global configuration command is:

```
dns-record a|ns dns_name ip_address {ttl_value {single|multiple
    {kal-ap-vip|kal-ap|kal-icmp|kal-none {ip_address2}}}}
```

The options and variables for this global configuration mode command are:

- **a|ns** - Indicates a request for an address record (a) or a name server record (ns).
- **dns_name** - Domain name mapped to the address record or name server record. Enter the name as a lowercase unquoted text string with no spaces and a maximum length of 63 characters.
- **ip_address** - IP address bound to the domain name within the DNS server zone. Enter the address in dotted-decimal notation (for example 172.16.6.7). This is the VIP for which a CSS client sends a **kal-ap-vip** request to itself or another CSS agent for load information.
- **ttl_value** - Optional Time to Live (TTL) value in seconds. This value determines how long the DNS client remembers the IP address response to the query. Enter a value between 0 to 65535. The default is 0.
- **single|multiple** - Optional number of records to return in a DNS response message. By default, the DNS server returns a single A-record. Specifying **single** returns one A- or NS-record. Specifying **multiple** returns two A- or NS-records.
- **kal-ap-vip** - Optional CSS keepalive message type keyword used by a CSS client to request load information for the VIP specified in the **ip_address** value from the CSS agent specified in the **ip_address2** value. Use this option to allow a CSS client to query a local or remote CSS agent for load information for a VIP configured on multiple content rules.
- **kal-ap** - Optional CSS keepalive message type keyword used by a CSS client to request load information for the domain specified in the **dns_name** variable from the CSS agent specified in the **ip_address2** value. Use this option to allow a CSS client to query a local or remote CSS agent for load information for a domain configured on a single content rule.



Note To use kal-ap proximity keepalive messages, lower-level CSSs acting as either data centers or DNS servers must be running the Enhanced feature set. When the Proximity Domain Name Server (PDNS) is directly attached to a server farm, an internal keepalive is used.

To obtain load information from local services only, use the **add dns record_name** command in the associated content rule. Refer to the *Cisco Content Services Switch Advanced Configuration Guide*.

- **kal-icmp** (default keepalive) - Optional keepalive message type keyword that specifies ICMP echo (PING).
- **kal-none** - Optional keepalive message type keyword that specifies no keepalive messaging.
- **ip_address2** - IP address of the local or remote CSS agent interface receiving CSS keepalive messages. If you omit this address while the keepalive type is specified, the CSS uses the DNS IP address to complete keepalive messaging.

For example:

```
(config)# dns-record a www.work.com 192.168.12.7 10 single kal-ap-vip 172.16.25.3
```

For details on the other **dns-record** command options and variables, refer to the *Cisco Content Services Switch Advanced Configuration Guide*.

Korean Certification Information

The following Korean certification information applies to the CSS 11000 series models. The certification label on the CSS model provides the applicable certification number.

- Trade Name or Applicant: Cisco Systems, Inc.
- Manufacturing Date: (To determine the date, see the explanation later in this section)
- Manufacturer/Nationality: Cisco Systems, Inc./USA

The Manufacturing Date year of the CSS model is embedded in the line of text under the Cisco serial number bar code. The line of text consists of 11 characters, similar to the following representation:

LLLYYWWSSSS

This fields provide:

- The location of the supplier (LLL)
- The year (YY) of manufacture
- The work week (WW)
- The sequential serial ID (SSSS)

The year is in a coded format. To determine the year of the Manufacturing Date, see [Table 4](#).

Table 4 *Manufacturing Date Code and Associated Year*

Code (YY)	Associated Year
01	1997
02	1998
03	1999
04	2000
05	2001
06	2002
07	2003

Cisco 11000 Series CSS Documentation Roadmap

This roadmap lists the documentation set that supports the Cisco 11000 series CSS. The documentation is available in the following forms:

- On the World Wide Web from the Cisco Systems home page (www.cisco.com)
- In print (see the following table for ordering information)


Note

You can obtain the most recent documentation for the Cisco 11000 series CSS on the following Web page: http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/css_500/index.htm.

Document Title	Description	Order Number ¹
<i>Cisco 11000 Series Content Services Switch Getting Started Guide</i>	Provides information for installing, cabling, and booting the CSS. In addition, this guide provides information about CSS specifications, cable pinouts, troubleshooting, and log messages.	DOC-7811766=
<i>Cisco Content Services Switch Basic Configuration Guide</i>	This guide describes how to perform a basic CSS configuration including logging into the CSS, upgrading your CSS software, and configuring: <ul style="list-style-type: none"> • The CSS for operation • User profile and CSS parameters • DNS, ARP, RIP, IP, and bridging features • Management ports, interfaces, and circuits • Services • Owners • Content rules 	DOC-7811424=

Document Title	Description	Order Number ¹
<i>Cisco Content Services Switch Advanced Configuration Guide</i>	Describes how to configure advanced CSS features, including: <ul style="list-style-type: none"> • Sticky parameters • HTTP header load balancing • Source groups, Access Control Lists (ACLs), Extension Qualifier Lists (EQLs), Uniform Resource Locator Qualifier Lists (URQLs), Network Qualifier Lists (NQLs), and Domain Qualifier Lists (DQLs) • VIP and CSS redundancy • Caching • Domain Name Service (DNS) • Demand-Based Content Replication and content staging and replication • Firewall Load Balancing • OSPF routing protocol • Network Proximity • CSS scripting language 	DOC-7811624=
<i>Cisco Content Services Switch Device Management User Interface Quick Start Guide</i>	Provides an overview on using the Device Management user interface, an HTML-based Web application that you use to configure and manage a CSS.	DOC-7813125=
<i>Cisco Content Services Switch Command Reference</i>	Provides an alphabetical list of all CSS Command Line Interface commands including syntax, options, and related commands.	DOC-7811425=

1. You can order printed versions of documents with DOC numbers.

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 “[Cisco 11000 Series CSS Documentation Roadmap](#)” section.



Copyright © 2002, Cisco Systems, Inc.
All rights reserved.