Release Note for the Cisco ACE Application Control Engine Module

January 23, 2012

Note The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note applies to the following software versions for the Cisco Application Control Engine Module (ACE), model ACE30 (ACE30_MOD_K9):

- A5(1.2)
- A5(1.1)
- A5(1.0)

For information on the ACE module features and configuration details, see the ACE documentation located at:

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

This release note contains the following sections:

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

New Software Features in Version A5(1.2)

Software version A5(1.2) provides the following new features:

IPv6 and IPv4 Route Support with Route Health Injection (RHI)

Per CSCtr24875 and CSCtr33704, software version A5(1.2) now enables the ACE module operating with the Catalyst 6500 series switch supervisor engine to support IPv6 **and** IPv4 routes for Route Health Injection (RHI) with Cisco IOS release 12.2(33)SXJ2 or later releases.

Dual Cisco Nexus 7000 Support

Per CSCtt42551, you may now configure up to two Cisco Nexus 7000 Series switches per ACE as a means to determine the locality of the VMs in the local and the remote data centers. Use the **nexus-device** command in configuration mode in the Admin context to create each local Cisco Nexus device on the ACE.

For example:

```
nexus-device otv-sw1
  ip-address 10.8.56.11
  credentials admin encrypted XyQhMSMkSU7LfCA3yn/KWHQYHHu/nFHMG0rbR8F02AfV

nexus-device otv-sw2
  ip-address 10.8.56.12
  credentials admin encrypted XyQhMSMkSU7LfCA3yn/KWHQYHHu/nFHMG0rbR8F02AfV
```

For details on how to configure a Cisco Nexus 7000 series switch to retrieve locality information for the dynamic workload scaling (DWS) feature, see the "Configuring the Nexus Device" section in Chapter 5, Configuring Dynamic Workload Scaling, of the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Ability to Back Up and Restore Only SSL Files Between ACEs

Per CSCtq38074, the ACE now allows you to specify to back up only SSL files from your ACE and restore all SSL files to the new device. The redundancy configuration on the standby ACE synchronizes the configuration from the active ACE to the standby ACE.

During the restore process, the ACE does not create the missing contexts. The restore functionality looks at each context in the backup file and if the context is present in the ACE, SSL files are restored. Otherwise, if the context does not exist, the restore process is skipped for this context. The restore process then continues with the next context in the backup file.

The modified syntax of the **backup** and **restore** Exec mode commands is as follows:

backup [**all**] [**pass-phrase** *text_string*] [**ssl-only**] [**exclude** *component*]

restore {[**all**] **disk0:***archive_filename*} [**pass-phrase** *text_string*] [**ssl-only**] [**exclude** {**licenses** | **ssl-files**}]

The optional **ssl-only** keyword has been added to the CLI syntax of the **backup** and **restore** commands to enableyou to specify exportable SSL files as part of the configuration file backup and restore processes. The nonexportable files are not supported by the back up operation and need to be restored manually.

Route Health Injection (RHI) Enhancement to Support a Layer 3 Firewall

Per CSCto55268, the **ip route inject vla**n command has been modified to allow you to specify the next-hop address to use on the Multilayer Switch Feature Card (MSFC) for the Catalyst 6500 series switch when there is a nontransparent Layer 3 firewall between the ACE and the MSFC.

The modified syntax of the **ip route inject vla**n Interface mode command is as follows:

ip route inject vlan *vlan_id* [*ip_address*]

no ip route inject vlan *vlan_id* [*ip_address*]

The arguments and options are as follows:

- *vlan_id*—Interface shared between the supervisor and the intervening device. Enter the ID as an integer from 2 to 4090.
- *ip_address*—(Optional) IP address to use on the MSFC as the next-hop address. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

For example, to specify the IP address on the MSFC as the next-hop address for VLAN 40, enter:

```
c6k1-ace30/Admin(config-if)# ip route inject vlan 40 10.10.10.10
c6k1-ace30/Admin(config-if)#
```

Default SSL Handshake Support (Per RFC 5746)

With defect CSCtd21177, a PSIRT case was initiated. An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.

RFC 5746 defines the renegotiation indication extension that allows SSL/TLS to perform SECURED renegotiation.

Per CSCtq48352, this enhancement supports a secure handshake by default on the ACE, as defined by RFC 5746. By default, the ACE now allows SECURED SSL/TLS renegotiation with a client and server that supports RFC 5746 and, by default, the ACE disallows UNSECURED SSL/TLS renegotiation with a client and server that do not support RFC 5746 (same as the previous behavior).

The following two new statistics have been added to the **show stats crypto server** and **show stats crypto client** commands:

- SSLv3 Secured Rehandshakes—Number of secured SSLv3 renegotiation handshakes that the ACE performed successfully with the client and server.
- TLSv1 Secured Rehandshakes—Number of secured TLSv1 renegotiation handshakes that the ACE performed successfully with the client and server.

Addition of the Normalization Stateless Function

The ACE uses TCP normalization to perform checks for Layer 4 packets that have invalid or suspect conditions. Per CSCtr31749, the **normalization stateless** command has been added to Interface mode primarily for use in DSR scenarios as well as a means to provide a certain level of protection against Distributed Denial of Service (DDoS) attacks on an interface when a TCP connection is created. The **normalization stateless** command is applicable only to Layer 4 flows.

Note The **normalization stateless** command is for DSR TCP connections only and does not apply to UDP stateless connections.

When you specify the **normalization stateless** command, the ACE processes TCP connections on an interface as stateless connections that undergo TCP normalization checks (for example, TCP window, TCP state, TCP sequence number, and other normalization checks).

Only SYN packets are allowed to create a TCP connection. When the connection is created, Layer 4 normalization checks are relaxed. In this case, because only a SYN packet is allowed to create a connection, the ACE sends a reset (RST) when the connection ends. The **no normalization stateless** command disables the function.

```
lbmb1104-11/CTX1(config)# interface vlan 461
lbmb1104-11/CTX1(config-if)# normalization stateless
```

With the **normalization stateless** command, there are no additional counters in the ACE used to track when a stateless DSR TCP connection is denied or DDoS-protected. All encountered issues are summarized under the existing counters available with the **show np** command output.

See the *Cisco Application Control Engine (ACE) Troubleshooting Guide* wiki for details on the **show np** command output:

show np 1 me-stats -snormalization

RADIUS-Attribute Sticky Group Enhancement

A RADIUS-attribute sticky group enables the ACE to stick client connections to the same real server based on a RADIUS attribute. By default, a sticky entry is always created when the ACE receives an Accounting Start packet regardless of the subsequent ACK. “Accounting only” customer deployments require sticky entries to be validated by a response (ACK). After the sticky entry is created, if the real server fails to respond to or acknowledge the request, all subsequent requests must be re-load balanced excluding this real server.

Per CSCtu04121, enhancements have been made to the RADIUS-attribute sticky group to optimize sticky entry creation for Accounting Only deployments during RADIUS load balancing. With this enhancement, a new option has been added in sticky RADIUS configuration mode (accessed through the **sticky radius framed-ip** command and the **sticky radius framed-ip username** command) to instruct the ACE to use a sticky entry only after it has been validated by a server response. In the case where no response has been received and the sticky entry has not been validated, the ACE will re-load balance, excluding the real server to which the RADIUS request was stuck initially.

At the end of the service delivery, the client generates an Accounting Stop packet that describes the type of service that was delivered and statistics (optional). The Accounting Stop packet deletes the sticky entry immediately without waiting for the ACK.

The new option in sticky RADIUS configuration mode is as follows:

wait-for-ack

Use the **no** form of this command to return operation to the default behavior.

For example, to create a group for RADIUS-attribute stickiness that includes the “wait for ACK” function, enter the following commands:

```
host1/Admin(config)# sticky radius framed-ip RADIUS_GROUP
host1/Admin(config-sticky-radius)# wait-for-ack
```

The **show sticky database detail** Exec mode command has also been modified to display the new RADIUS Wait-For-Ack entry. The states of this entry are either True or False.

For example, enter the following command:

```
host1/Admin# show sticky database detail
processor (0/3):             3
results index:               1 of 1
sticky group:                fip-uname-farm
sticky type:                 RADIUS
rserver:                     rs-01
realPort:                    0
timeout (secs):              86400
sticky-entry:                0x1b6e0438e29341a
internal entry-id:           0xc020000b
time-to-expire (secs):       86342
sticky-hit-count:            1
active-conn-count:           0
in-use reference count:      0
static entry:                FALSE
reverse entry:               FALSE
active entry:                TRUE
timeout-active-conns:        FALSE
```

```
created-from-HA-peer:        FALSE
HA-replicated-at-least-once: TRUE
Radius Wait-For-Ack:         TRUE <<<<<<

Total Sticky Entries: 1
```

Globally Applying Parameter Map Inactivity and TCP Half-Closed Connection Timeout Values

Per CSCtl97681, you can globally apply the inactivity and TCP half-closed connection timeout values of a connection parameter map in a context. The global timeout values override the default values for all the Layer 3 rules in the context. If you configure the timeout values for a specific parameter map, they override the global inactivity timeout values.

Before you can globally apply the connection timeout values, you must configure a connection parameter map that contains these values. You can configure this parameter map with either or both the inactivity and TCP half-closed connection timeouts. For example, to configure a connection parameter map with the inactivity and half-closed connection timeouts, enter the following:

```
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)# set timeout inactivity 7200
host1/Admin(config-parammap-conn)# set tcp timeout half-closed 1800
```

You cannot configure any additional parameters to this parameter map. If the parameter map is configured with parameters other than these connection timeouts, the ACE displays the following error message:

```
Error: Parameter map can't be applied globally.
```

After you configure the parameter map, you can globally apply it and its timeouts through the **connection advanced-option default-override** command in configuration mode. The syntax of the command is as follows:

connection advanced-option default-override *connection_parameter_map*

The *connection_parameter_map* argument is the name of the connection parameter map name configured with the inactivity or half-closed connection timeout values. For example, enter the following:

```
host1/Admin(config)# connection advanced-option default-override TCP_MAP
```

The **show service-policy** command indicates the global parameter map applied to the Layer 3 rule by appending the (Global) tag to its name. The **show parameter map** command displays the globally-applied inactivity and half-closed connection timeouts by appending the (Global) tag appended to the timeout values.

To remove the global timeout values, enter the following:

```
host1/Admin(config)# no connection advanced-option default-override TCP_MAP
```

Increase in the HTTP Load-Balancing Limitation

Per CSCtn14041, the HTTP load-balancing limitation of 1024 entries per class map and 1024 entries per policy map has increased to 4096. The line number value for match statements has increased from 1024 to 4096.

CLI Support for Connections Per Second (CPS) at the Virtual Server Level

Per CSCtn73488, the **show service-policy** command now includes the conns per second field that displays the connections per second at the virtual server level when you configure more than one VIP under a class map. When you configure one VIP under a class map, the connections per second field is displayed at the VIP level.

For example:

```
switch/Admin# show service-policy L7_policy

Status     : ACTIVE
------------------------------------------
Interface: vlan 725 727
  service-policy: httJG
    class: vip-JG
      loadbalance:
        L7 loadbalance policy: L7_policy
        Regex dnld status    : SUCCESSFUL
        VIP Route Metric     : 77
        VIP Route Advertise  : DISABLED
        VIP ICMP Reply       : ENABLED
        VIP State: INSERVICE
        VIP DWS state: DWS_DISABLED
        Persistence Rebalance: ENABLED
        curr conns       : 0         , hit count        : 1647936
        dropped conns    : 1632955
        conns per second    : 50    >>>>>>>>>>>>>>>>>>>>>>>>>>>> This stat has been added
        client pkt count : 4972447   , client byte count: 459647112
        server pkt count : 80791     , server byte count: 7090355
        conn-rate-limit      : 100       , drop-count : 22522
        bandwidth-rate-limit : -         , drop-count : -
      compression:
        bytes_in  : 0                          bytes_out : 0
        Compression ratio : 0.00%
                Gzip: 0               Deflate: 0
      compression errors:
        User-Agent  : 0               Accept-Encoding    : 0
        Content size: 0               Content type       : 0
        Not HTTP 1.1: 0               HTTP response error: 0
        Others      : 0
        Parameter-map(s):
          con
```

Mitigating a Slowloris HTTP DoS Attack

Slowloris is an HTTP Denial of Service (DoS) tool written in PERL that is used to perform denial of service attacks against Apache-based servers (as well as other web services). Slowloris exhausts all available server connections by repeatedly initiating several hundred valid HTTP requests to the server and keeping these connections open using a minimal amount of TCP traffic to consume server resources. Once server resources are exhausted, the server is no longer able to respond to legitimate traffic.

Per CSCtu08459, you are now able to configure the ACE to mitigate a Slowloris HTTP DOS attack by including an HTTP parse timeout in your HTTP parameter map. With software version A5(1.2), the new **set max-parse-time** command has been added as protection from Slowloris DoS attacks. The default HTTP parsing timeout is set to 255 seconds, and if the ACE does not receive a GET request from the connection within 255 seconds, the HTTP parse timeout initiates and the ACE drops the connection and sends a reset to the client. You can increase this timeout maximum through the **set max-parse-time** command.

The syntax of this parameter map HTTP configuration mode command is as follows:

set max-parse-time *time*

The *time* argument is the time in seconds for the maximum length of the HTTP parsing timeout. Valid entries are 1 to 65535 seconds.

For example, to enter an HTTP parsing timeout of 200 seconds, enter the following:

```
host1/Admin(config)# parameter-map type http HTTP_MAP
host1/Admin(config-parammap-http)# set max-parse-time 200
```

Closing a TCP Connection in a FIN_WAIT State

You may be operating in an environment where connections do not close due to clients that fail to reply to a FIN from one or more real servers. This situation can result in the server continuing to handle the open connections (remaining in a FIN_WAIT_1 state), which, during high volume traffic, can result in the server running out of connections. As a result, the server maintains a high CPU load because it continues to wait for a FIN, ACK, or RST to close the connection. The server is unable to answer requests because it is handling the open connections.

Per CSCtr61749, the ACE now supports the ability to define a timeout in your connection parameter map for TCP connections that are in the FIN_WAIT_I state. The **set tcp timeout** command now includes the **fast-fin** option to specify the FIN timeout (in seconds). This command is available in the Admin context only.

The syntax of this parameter map connection configuration mode command is as follows:

set tcp timeout fast-fin *time*

The *time* argument is the time in seconds after which the ACE will send a timeout for TCP connections that are in a FIN_WAIT_1 state. Enter an integer from 1 to 4294967295. The default is no FIN timeout.

For example, to set a FIN timeout of 200 seconds, enter the following:

```
host1/Admin(config)# parameter-map type connection conn_para
host1/Admin(config-parammap-http)# set tcp timeout fast-fin 60
```

To return to the default state of no FIN timeout, enter the following:

```
host1/Admin(config-parammap-http)# no set max-parse-time
```

The **show parameter-map** command output now includes information on the state of the fast FIN timeout, as shown below:

```
switch/Admin#  show parameter-map

 Number of parameter-maps : 2

 Parameter-map : CONN_MAP
 Description : -
 Type : connection
    nagle                              : disabled
    slow start                         : disabled
    buffer-share size                  : 32768
    inactivity timeout (seconds)       : 240
    reassembly timeout (seconds)       : 60
    embryonic timeout (seconds)        : 5
    ack-delay (milliseconds)           : 200
    WAN Optimization RTT (milliseconds): 65535
    half-closed timeout (seconds)      : 3600
    fast FIN timeout (seconds)         : disabled >>>>>>>>>>>>> This field has been added
    TOS rewrite                        : disabled
    syn retry count                    : 4
    TCP MSS min                        : 0
    TCP MSS max                        : 1460
    tcp-options drop range             : 0-0
    tcp-options allow range            : 0-0
    tcp-options clear range            : 1-255
    selective-ack                      : clear
    timestamp                          : clear
    window-scale                       : clear
    window-scale factor                : 0
    reserved-bits                      : allow
    random-seq-num                     : enabled
    SYN data                           : allow
    exceed-mss                         : drop
    urgent-flag                        : allow
    conn-rate-limit                    : disabled
    bandwidth-rate-limit               : disabled
```

Selecting an HTTPS Certificate and Key

Secure (SSL) Hypertext Transfer Protocol (HTTPS) is used by the ACE module to send and receive XML documents between the ACE and an NMS through port 443.

Per CSCte42757, the ACE allows you to specify the certificate and key that the ACE HTTP server uses during the Secure Sockets Layer (SSL) handshake. This enhancement has been provided to allow you to use your own signed certificates for the ACE.

The syntax of this configuration mode command is as follows:

ip https certificate *cert-name key-name*

The arguments are as follows:

- *cert-name*—Specifies the name of an existing certificate file loaded on the ACE. To list all available certificates loaded on the ACE, include the question mark (?) character after the **ip https certificate** command. For example:

```
host1/Admin(config)# ip https certificate ?
  cisco-sample-cert
  mycert.crt
```

- *key-name*—Specifies the name of an existing key pair file loaded on the ACE. To list all available keys loaded on the ACE, include the question mark (?) character after the **ip https certificate** *cert-name* command. For example:

```
host1/Admin(config)# ip https certificate mycert.crt ?
  cisco-sample-key
  mykey.key
```

Use the **no** form of this command to restore the default certificate.

Note the following usage considerations with selecting an HTTPS certificate and key:

- The **ip https certificate** command is available in the Admin context only.
- When you select the public key to be embedded in the certificate, ensure that it matches the public key in the key pair file that you select. The ACE warns you if there is a mismatch by displaying the following error message: “Error: Mismatched key/cert pair”. To verify that the public keys in the two files match, use the **do crypto verify** command from configuration mode.
- Use the **show ip https** command to display the current HTTP server configuration information.

For example, to specify a certificate and key for the HTTPS server on the ACE, enter the following command:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z.
host1/Admin(config)# ip https certificate MYCERT.PEM MYKEY.PEM
```

To reset the certificate and key on the HTTPS server, enter the following command:

```
host1/Admin(config)# no ip https certificate
```

Related SNMP Changes for A5(1.2)

Per CSCto13407, the ACE provides SNMP support for the slbVServerConnectionRate OID. This OID was added to the slbVServerInfoTable table and indicates the connections per second for the virtual server.

Per CSCtl73658, the following two new MIB objects have been added to the CISCO-SLB-EXT-MIB to better track Layer 7 parsing failures:

- cslbxStatsL7ParserErrorRejects
- cslbxStatsMaxParseLenReject

The two new MIB objects are part of cslbxStatsTable.

Included below is a summary of the SNMP OIDs for these two objects:

- cslbxStatsMaxParseLenRejects OBJECT-TYPE:

  SYNTAX Counter32

  UNITS "connections"

  MAX-ACCESS read-only

  STATUS current

DESCRIPTION

"The number of connections rejected because the length of an HTTP request or response header exceeded the maximum L7 parse length configured for the matching virtual server."

::= { cslbxStatsTableEntry 18 }

- cslbxStatsL7ParserErrorRejects OBJECT-TYPE:

  SYNTAX Counter32

  UNITS "connections"

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "The number of connections rejected because an error occurred while parsing the connection data at Layer 7."

  ::= { cslbxStatsTableEntry 20 }

New Software Features in Version A5(1.0)

The A5(1.0) software release provides the following new features:

- Dual stack:
  - IPv4-to-IPv4 and IPv6-to-IPv6
  - HTTP and DNS inspection for native IPv6-IPv6 traffic
- Translation:
  - SLB64, SLB46 for all Layer 4 load balancing which do not require payload modifications or pinholes
  - NAT64, NAT46 for all TCP and UDP protocols which do not need payload modifications or pinholes
  - SLB64 and SLB46 support for Layer 7 load balancing for HTTP and SSL protocols.
  - No DNS64 or DNS46 support on ACE
- Mixed IPv4 and IPv6 real server support
- IPv6 addressing, including link-local, global unicast, unique local, peer, and alias addresses.
- IPv6 protocol support:
  - Neighbor Discovery (ND)
  - Router Discovery (RD)
  - Duplicate Address Detection (DAD)
  - ICMPv6
  - DHCPv6
- Application awareness: HTTP, HTTPS, and DNS
- Online Certificate Status Protocol (OCSP) support for authenticating Secure Sockets Layer (SSL) offloaded sessions for both IPv6 and IPv4

Chassis, Supervisor Engine, and Cisco IOS Support for the ACE30 Module

Table 1 and Table 2 summarize the chassis, supervisor engine model, and Cisco IOS version support for the ACE30 module in the Catalyst 6500E series switch and the Cisco 7600 series router, respectively.

Table 1 Chassis, Supervisor Engine, and Cisco IOS Support for the ACE 30 in a Catalyst 6500 Series Switch with a Multilayer Switch Feature Card (MSFC3 or Later)

Catalyst 6500 Series Switch Chassis	Supervisor Engine Model	Minimum Required Cisco IOS Version
6503-E	VS-S2T-10G [3]	15.0(1)SY (or later)
6504-E	VS-S2T-10G-XL	
6506-E	WS-SUP720-3B	12.2(33)SXI4 or later releases
6509-E[1]	WS-SUP720-3BXL	
6509-V-E	VS-S720-10G-3C(=)	
6513	VS-S720-10G-3CXL(=)	
6513-E[2]		

1. The Catalyst 6509-E chassis supports up to six ACE 30 modules with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), and running Cisco IOS software version 15.0(1)SY1 (or later) with ACE module software version A5(1.2).
2. The Catalyst 6513-E chassis supports up to nine ACE 30 modules with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), and running Cisco IOS software version 15.0(1)SY1 (or later) with ACE module software version A5(1.2).
3. The minimum required ACE30 module software version for Supervisor Engine 2T support is A5(1.1) or later. This software version supports both supervisor engine models: VS-S2T-10G and VS-S2T-10G-XL.

Table 2 Cisco Supervisor Engine, Route Switch Processor (RSP), and Cisco IOS Support for the ACE30 in a Cisco 7600 Series Router with a Multilayer Switch Feature Card (MSFC3 or Later)

Cisco 7600 Series Router Chassis	Supervisor Engine or RSP	Minimum Required Cisco IOS Version
7603	WS-SUP720-3B	15.0(1)S or later releases
7604	WS-SUP720-3BXL	
7609	RSP720-3C-GE(=)	
7613	RSP720-3CXL-GE(=)	
7603-S	RSP720-3C-10GE	
7604-S	RSP720-3CXL-10GE	
7606-S		
7609-S		

Virtual Switching System Support

The ACE30 running ACE software version A4(1.0) or later releases and installed in a Catalyst 6500 series switch running Cisco IOS release 12.2(33)SXI4 or later releases support the Virtual Switching System (VSS). VSS is a system virtualization technology that allows the pooling of multiple Catalyst 6500 switches into a single virtual switch for increased operational efficiency by simplifying the network. Inter-chassis Supervisor switchover (SSO) boosts non-stop communication. For more information about VSS, see the *Cisco IOS Version 12.2(33)SXI4 Configuration Guide*.

Route Health Injection (RHI) Support for the ACE Module with the A5(1.x) Software Releases

Note the following ACE module support for Route Health Injection (RHI) with the A5(1.x) software releases:

- With software release A5(1.2), the ACE module operating with the Catalyst 6500 series switch supervisor engine supports both IPv6 and IPv4 routes for Route Health Injection (RHI) with Cisco IOS release 12.2(33)SXJ2 or later releases.
- With software releases A5(1.0) and A5(1.1), the ACE module operating with the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine supports only IPv4 routes for Route Health Injection (RHI) with Cisco IOS release 12.2(33)SXI4 or later releases. RHI for IPv6 routes is not supported at this time. You will not encounter this issue with RHI for IPv4 routes. See CSCtr14599, CSCtr24875, CSCtr33704 in this release note for additional A5(1.0)-related information on this issue.

ACE Operating Considerations

The ACE operating considerations are as follows:

- Starting with software version A4(1.0), the default connection inactivity timeout settings for the ACE have changed to the following values:
  - ICMP—2 seconds
  - TCP—3600 seconds (1 hour)
  - HTTP/SSL—300 seconds
  - UDP—10 seconds

  The default HTTP and SSL ports (80 and 443) now have a default inactivity timeout of 300 seconds.
- Starting with software version A4(1.0), it is no longer necessary to configure a resource class in the Admin context to allocate resources for stickiness. You can still allocate sticky resources if you wish, but skipping this step will not affect sticky functionality.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A2(3.0) to A4(1.0) or later, bulk sync, dynamic incremental sync, and connection replication are automatically disabled only while the active ACE is running software version A4(1.0) or later and the standby ACE is running software version A2(3.0). See Table 3.

We recommend that you do not make any configuration changes during this time and that you do not keep the ACEs in this state for an extended period of time. However, if you must make configuration changes while the ACEs are in split mode, ensure that you manually synchronize to the standby ACE any configuration changes that you make on the active ACE. After you complete the software upgrade of both ACEs, a bulk sync occurs automatically to replicate the entire configuration of the new active ACE to the new standby ACE. At this time, dynamic incremental sync will be enabled again. For details about config sync, see Chapter 6, “Configuring Redundant ACEs” in the *Administration Guide, Cisco ACE Application Control Engine*.

Table 3 Redundancy Feature Availability Between Major ACE Software Versions

Platform	Active	Standby	Bulk Sync	Incr Sync	Conn Repl	Sticky Repl	Operation	Comments
Module	A2(x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A4(1.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A4(2.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A5(x)	A2(x)	No	No	No	No	Downgrade	Functionality not supported due to architectural differences between the ACE20 and the ACE30 hardware
Module	A5(x)	A4(1.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Module	A5(x)	A4(2.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4

- During an upgrade to software version A4(1.0) or later in a redundant configuration, we recommend that you do not run the two ACEs with different versions of software (split mode) for an extended period of time. However, if you must remain in split mode for a period of time to make configuration changes, we strongly recommend that you disable configuration synchronization (config sync) by entering the following command:

  ```
  host1/Admin(con)# no ft auto-sync running-config
  ```

  When you have finished making configuration changes to the active ACE, reenable config sync by entering the following command:

  ```
  host1/Admin(con)# ft auto-sync running-config
  ```

  After you reenable config sync, the ACE automatically synchronizes the configuration changes from the active ACE to the standby ACE.
- We strongly recommend that you do not make any CLI changes when the ACE modules in a redundant configuration are running different software versions. Unexpected results may occur. Remove any new feature commands before performing a downgrade on the ACE.
- In software version A4(1.0) or later, all four of the network processors (NPs) must transition into the retcode or inband failed state before the ACE marks the real server as RETCODE-FAILED or INHAND-HM-FAILED, respectively, and places it on the reactivate list for recovery. This is also true for the maxconn limit, where the threshold values are divided among all four NPs similar to the retcode and inband failed states. The real servers will move to the MAXCONN state only when all four NPs reach the MAXCONN state.

Note that the following may occur:

- When some NPs are in the retcode failed state and the other NPs are in the inband failed state due to a traffic pattern that hashes connections to specific NPs, the real servers are in the OPERATIONAL state as displayed by the **show serverfarm** *name* command because the NPs are deadlocked waiting until the other NPs reach the retcode or inband failed state, respectively.
- When some NPs are in the retcode or inband failed state due to a traffic pattern that hashes only to some NPs and not to the other NPs, the real servers are left in the OPERATIONAL state until all NPs transition into the retcode or inband failed state, respectively.

When the traffic distribution is uniform across all NPs, these issues do not occur.

- The ACE requires a route back to the client before it can forward a request to a server. If the route back to the client is not present, the ACE cannot establish a flow and drops the client request. Make sure that you configure the appropriate routing to the client network on the ACE VLAN where the client traffic enters the ACE module.
- When you downgrade the ACE software, the features and commands of the higher release are lost because they are not supported by the lower release.
- When redundant ACEs lose connectivity (for example, because of a network interruption) and they attempt to reestablish their connection, if you enter the **show ft peer** or **show ft group** command during this time, the response to this command may be delayed.
- If you are using the Application Networking Manager (ANM) to manage an ACE module and you configure a named object at the ACE CLI, ANM does not support all of the special characters that the ACE CLI supports for a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

  When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on) for use with ANM, enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.
- When you remove a NAT pool configuration, wait more than five seconds before adding a NAT pool with the same ID.
- The Account Expiry field for the **show user-account** command displays the date, if any, when the user account expires. This date is based on Coordinated Universal Time (UTC/GMT) which the ACE keeps internally. If you use the **clock timezone** command to configure a UTC offset, this field displays the UTC date and does not reflect the date with the offset as displayed by the **show clock** command.

Available ACE Licenses

By default, the ACE supports virtualization with one Admin context and five user contexts, 4 gigabits per second (Gbps) module bandwidth, 1 Gbps compression, and 1,000 SSL transactions per second (TPS). You can increase the number of default user contexts, module bandwidth, and SSL TPS by purchasing the licenses shown in Table 4.

Table 4 ACE30 License Bundles

License Bundle	Product ID (PID)	License File	Description
Base (default)	ACE30-BASE-04-K9	None required	4 Gbps bandwidth 1 Gbps compression 1,000 SSL TPS 5 Virtual Contexts
Base to 4 Gbps 4 Gbps Bundle	ACE30-MOD-UPG1= ACE30-MOD-04-K9	ACE30-MOD-UPG1 ACE30-MOD-04-K9	4 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 Virtual Contexts
4 Gbps to 8 Gbps 8 Gbps Bundle	ACE30-MOD-UPG2= ACE30-MOD-08-K9	ACE30-MOD-UPG2 ACE30-MOD-08-K9	8 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 virtual contexts
8 Gbps to 16 Gbps 16 Gbps Bundle	ACE30-MOD-UPG3= ACE30-MOD-16-K9	ACE30-MOD-UPG3 ACE30-MOD-16-K9	16 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 virtual contexts

You can also obtain an ACE demo license for each license bundle. You can get a demo license that is valid for 30 or 90 days. At the end of this period, you will need to update the demo license with a permanent license to continue to use the ACE software. To view the expiration of the demo license, use the **show license usage** command in Exec mode. If you need to replace the ACE module, you can copy and install the licenses onto the replacement module.

Note You can access the **license** and **show license** commands only in the Admin context. You must have the Admin role in the Admin context to perform the tasks of installing, removing, and updating the license.

Ordering an Upgrade License and Generating a License Key

This section describes the process to order an upgrade license and to generate a license key for your ACE. To order an upgrade license, perform the following steps:

Step 1 Order one of the licenses from the list in the "Obtaining Documentation and Submitting a Service Request" section using any of the available Cisco ordering tools on Cisco.com.

Step 2 When you receive the Software License Claim Certificate from Cisco, follow the instructions that direct you to the cisco.com website. As a registered user of cisco.com, go to this URL:

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

Step 3 Enter the Product Authorization Key (PAK) number found on the license certificate as your proof of purchase.

Step 4 Provide all the requested information to generate a license key.

Step 5 After the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions. Save the license key e-mail in a safe place in case you need it in the future (for example, to transfer the license to another ACE).

For information about installing and managing ACE licenses, refer to Chapter 3, Managing ACE Software Licenses, in the *Administration Guide, Cisco ACE Application Control Engine*.

Upgrading Your ACE Module Software in a Redundant Configuration

To upgrade your ACE software from version A2(3.x) or A2(1.6a) or later to version A5(1.x), you must also migrate your ACE10 or ACE20 module to a new ACE30 module. For details about migrating to an ACE30 and upgrading your software to A4(1.0) or later, see the procedure in the *Installation Note, Cisco ACE Application Control Engine ACE30 Module*.

To upgrade your ACE software from A4(1.x) or A4(2.x) to version A5(1.x), the procedure in the following section assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the upgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

This section includes the following topics:

Before You Begin

Before you upgrade your ACE software, be sure that your ACE configurations meet the upgrade prerequisites in the following sections:

- Changing the Admin Password
- Changing the www User Password
- Creating a Checkpoint
- Copying the Startup Configuration of Each Context

Note If you are upgrading a redundant configuration from software version A4(1.x) or A4(2.x) to software version A5(1.x), while the two ACEs are in split mode with the earlier software version running on the active ACE and software version A5(1.x) running on the standby, config sync is disabled. If you make any configuration changes on the active ACE during this time, your changes are not synchronized to the standby and are lost. After you complete the upgrade, config sync is automatically reenabled. We recommend that you do not make any configuration changes while the two ACEs are in split mode.

Changing the Admin Password

Before you upgrade your ACE software, you **must** change the default Admin password if you have not already done so. Otherwise, after you upgrade the ACE software, you will only be able to log in to the ACE through the console port or through the supervisor engine of the Catalyst 6500 series switch or the Cisco 7600 series router.

For details on changing the default Admin password, see Chapter 1, Setting Up the ACE, in the *Administration Guide, Cisco ACE Application Control Engine*.

Changing the www User Password

Before you upgrade the ACE software, you **must** change the default www user password if you have not already done so. Otherwise, after you upgrade the ACE software, the www user will be disabled and you will not be able to use Extensible Markup Language (XML) to remotely configure an ACE until you change the default www user password.

For details on changing a user account password, see Chapter 2, Configuring Virtualization, in the *Virtualization Guide, Cisco ACE Application Control Engine*. In this case, the user would be **www**.

Caution If you do not change the www user password prior to upgrading the ACE software, configuration synchronization may fail and the context may not be in the STANDBY_HOT state.

Creating a Checkpoint

We strongly recommend that you create a checkpoint of the running-configuration of each context in your ACE. A checkpoint creates a snapshot of your configuration that you can later roll back to in case a problem occurs with an upgrade and you want to downgrade the software to a previous release. Use the **checkpoint create** command in Exec mode in each context for which you want to create a configuration checkpoint and name the checkpoint. For details about creating a checkpoint and rolling back a configuration, see the *Administration Guide, Cisco ACE Application Control Engine*.

Copying the Startup Configuration of Each Context

In addition to creating a checkpoint of the running-configuration of each context in your ACE, we also strongly recommend that you copy the startup configuration of each context to either:

- The disk0: file system on your ACE.
- An TFTP, FTP, or SFTP server.

Having a backup of the startup configuration of each context ensures that you can recover your ACE should an issue arise during the upgrade procedure. In that case, you can then downgrade and restore the existing startup configuration to your ACE.

Upgrade Procedure

To upgrade your ACE software in a redundant configuration, follow these steps:

Note Ensure that the preempt command is disabled before the upgrade procedure begins.

Step 1 Log in to both the active and standby ACEs. The Exec mode prompt appears at the CLI. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the Admin context. If necessary, log directly in to, or change to the Admin context.

```
ACE-1/Admin#
```

Step 2 Save the running configurations of every context by entering the **write memory all** command in Exec mode in the Admin context of each ACE.

```
ACE-1/Admin# write memory all
```

Step 3 Create a checkpoint in each context of both ACEs by entering the **checkpoint create** command in Exec mode.

```
ACE-1/Admin# checkpoint create ADMIN_CHECKPOINT
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint create C1_CHECKPOINT
```

Step 4 Copy the new software image to the image directory of each ACE (active and standby) by entering the **copy ftp**, **copy sftp**, or the **copy tftp** command in Exec mode. For example, to copy the image with the name c6ace-t1k9-mz.A5_1_0.bin through FTP, enter:

```
ACE-1/C1# changeto Admin
ACE-1/Admin# copy ftp://server1/images//c6ace-t1k9-mz.A5_1_0.bin image:
Enter source filename[/images/c6ace-t1k9-mz.A5_1_0.bin]?
Enter the destination filename[]? [c6ace-t1k9-mz.A5_1_0.bin] File already exists, do you
want to overwrite?[y/n]: [y]
Enter hostname for the ftp server[server1]?
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin] Enable Passive mode[Yes/No]: [Yes] no
Password:
```

Step 5 Ensure that the new software image is present on both the active and standby ACEs by entering the **dir** command in Exec mode. For example, enter:

```
ACE-1/Admin# dir image:c6ace-t1k9-mz.A5_1_0.bin
35913728  Oct 25 2010 01:17:01 c6ace-t1k9-mz.A5_1_0.bin

          Usage for image: filesystem
                 828182528 bytes total used
                  54165504 bytes free
                 882348032 bytes total
```

Step 6 Verify the current BOOT environment variable and configuration register setting by entering the **show bootvar** command in Exec mode. For example, enter:

```
ACE-1/Admin# show bootvar
BOOT variable = "image:c6ace-t1k9-mz.A5_1_0.bin"
Configuration register is 1
```

Step 7 Remove the existing image from the boot variable on ACE-1 by entering the **no boot system image:***ACE_image* command in configuration mode. For example, to remove the A4(1.0) image, enter:

```
ACE-1/Admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
```

```
ACE-1/Admin(config)# no boot system image:c6ace-t1k9-mz.A4_1_0.bin
```

Step 8 Configure ACE-1 to autoboot from the latest ACE image. To set the boot variable and configuration register to1 (perform auto boot and use startup-config file), use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin(config)# boot system image:c6ace-t1k9-mz.A5_1_0.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin# show bootvar
BOOT variable = "image:c6ace-t1k9-mz.A5_1_0.bin"
Configuration register is 1
```

Step 9 On the standby ACE module (ACE-2), perform the following:

- Enter the **show running-config** command and ensure that all the changes made in the active ACE (ACE-1) are also reflected on the standby ACE.
- Enter the **show bootvar** command to verify that the boot variable was synchronized with ACE-1.

Step 10 Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Upgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the **reload** command in Exec mode.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

After ACE-2 boots up, it may take a few minutes to reach the STANDBY_WARM state again. Configuration synchronization is still enabled and the connections through ACE-1 are still being replicated to ACE-2.

Note We do not recommend that you make any changes to the ACE-1 configuration. At this point in the upgrade procedure with ACE-2 in the STANDBY_WARM state, any incremental commands that you add to the ACE-1 configuration may not be properly synchronized to the ACE-2 configuration. To make any changes to ACE-1, disable incremental sync on ACE-1 and manually synchronize the changes to ACE-2.

Step 11 After the standby ACE reboots, log in and perform the following actions to verify the state of the standby ACE:

- Enter the **show version** command in Exec mode to verify that the module has properly rebooted with the latest ACE software image.
- Enter the **show ft group detail** command in Exec mode to verify that the standby ACE has recovered to a STANDBY_WARM state.

Step 12 Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes mastership of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

Step 13 Upgrade ACE-1 by reloading it. Verify that ACE-1 enters the STANDBY_WARM state (this action may take several minutes) by entering the **show ft group detail** command in Exec mode.

Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts mastership after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE once again.

```
ACE-1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

Step 14 Verify that ACE-1 is in the ACTIVE state and ACE-2 is in the STANDBY_WARM state by entering the **show ft group detail** command in Exec mode.

Downgrading Your ACE Module Software in a Redundant Configuration

If you need to downgrade your ACE software from version A5(1.x) to an earlier supported ACE software version (version A2(3.x) or A2(1.6a) or later), use the procedure in the *Installation Note, Cisco ACE Application Control Engine ACE30 Module*.

If you need to downgrade your ACE software from version A5(1.x) to either software version A4(2.x) or A4(1.x), use the procedure that follows. This procedure assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the downgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

Before You Begin

Before you downgrade your ACE software, ensure that the following conditions exist:

- Identical versions of the previous software image resides in the image: directory of both ACEs.
- The active ACE has a higher priority than the standby ACE and **preempt** is enabled on the FT group if you want the active ACE to remain active after the downgrade procedure.

Downgrade Procedure

To downgrade your A5(1.x) software to either software version A4(2.x) or A4(1.x) in a redundant configuration, perform these steps:

Step 1 If you have previously created checkpoints in your running-configuration files (highly recommended), roll back the configuration in each context on each ACE to the check-pointed configuration. For example:

```
ACE-1/Admin# checkpoint rollback CHECKPOINT_ADMIN
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint rollback CHECKPOINT_C1
```

Do the same on the other ACE. For information about creating checkpoints and rolling back configurations, see the *Administration Guide, Cisco ACE Application Control Engine*.

Step 2 Configure ACE-1 to automatically boot from the earlier ACE software image. To set the boot variable and configuration register to 1, use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin# config
ACE-1/Admin(config)# boot system image:c6ace-t1k9-mz.A4_1_0.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
```

```
ACE-1/Admin#
```

You can set up to two images through the **boot system** command. If the first image fails, the ACE tries to boot from the second image.

Step 3 Verify that the boot variable was synchronized to ACE-2 by entering the following command on ACE-2:

```
ACE-2/Admin# show bootvar
BOOT variable = "disk0:c6ace-c6ace-t1k9-mz.A4_1_0.bin"
Configuration register is 1
host1/Admin#
```

Step 4 Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Downgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the **reload** command.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

When ACE-2 loads the startup-configuration file, you may observe a few errors if you did not roll back the configuration to a checkpoint. These errors are harmless and occur because the ACE software does not recognize the A5(1.x) commands in the startup-configuration file.

Note Dynamic incremental sync is automatically disabled while the active ACE is running software version A5(1.x) and the standby ACE is running software version A4(2.x) or A4(1.x).

Step 5 Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes mastership of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

Step 6 Reload ACE-1 with the same ACE software version as ACE-2. Again, you may observe a few errors as ACE-1 loads the startup-configuration file.

```
ACE-1/Admin# reload
```

After ACE-1 boots up, it assumes the role of standby and enters the STANDBY_HOT state (this may take several minutes). You can verify the states of both ACEs by entering the **show ft group detail** command in Exec mode. Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts mastership after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE once again.

Step 7 Enter the **write memory all** command in both ACEs to save the running-configuration files in all configured contexts to their respective startup-configuration files. This action will eliminate future errors when the ACEs reload their startup-configuration files.

ACE Documentation Set

You can access the ACE module documentation on www.cisco.com at:

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

For information about installing the ACE module hardware, see the following documents on Cisco.com:

Document Title	Description
Installation Note, Cisco ACE Application Control Engine ACE30 Module	Provides information for installing the ACE module into the Catalyst 6500 series switch or a Cisco 7600 series router.

To familiarize yourself with the ACE module software, see the following documents on Cisco.com:

Document Title	Description
Release Note for the Cisco Application Control Engine Module	Provides information about operating considerations and caveats for the ACE.
Getting Started Guide, Cisco ACE Application Control Engine Module	Describes how to perform the initial setup and configuration tasks for the ACE module.

In addition to this document, the ACE module software documentation set includes the following:

Document Title	Description
Administration Guide, Cisco ACE Application Control Engine	Describes how to perform the following administration tasks on the ACE: • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
Cisco Application Control Engine (ACE) Configuration Examples Wiki	Provides examples of common configurations for load balancing, security, SSL, routing and bridging, virtualization, and so on.
Cisco Application Control Engine (ACE) Troubleshooting Wiki	Describes the procedures and methodology in wiki format to troubleshoot the most common problems that you may encounter during the operation of your ACE.

Document Title	Description
Command Reference, Cisco ACE Application Control Engine	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
Cisco CSM-to-ACE Conversion Tool User Guide	Describes how to use the CSM-to-ACE module conversion tool to migrate Cisco Content Switching Module (CSM) running- or startup-configuration files to the ACE.
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.
Routing and Bridging Guide, Cisco ACE Application Control Engine	Describes how to perform the following routing and bridging tasks on the ACE: • VLAN interfaces • IPv6, including transitioning IPv4 networks to IPv6, IPv6 header format, IPv6 addressing, and supported protocols • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)
Security Guide, Cisco ACE Application Control Engine	Describes how to perform the following ACE security configuration tasks: • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Translation (NAT)
Server Load-Balancing Guide, Cisco ACE Application Control Engine	Describes how to configure the following server load-balancing features on the ACE: • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Dynamic workload scaling (DWS) • Firewall load balancing • TCL scripts

Document Title	Description
SSL Guide, Cisco ACE Application Control Engine	Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
System Message Guide, Cisco ACE Application Control Engine	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.
Virtualization Guide, Cisco ACE Application Control Engine	Describes how to operate your ACE in a single context or in multiple contexts.

For detailed configuration information on the Cisco Application Networking Manager (ANM), see the following software document on Cisco.com:

User Guide, Cisco Application Networking Manager	Describes how to use Cisco Application Networking Manager (ANM), a networking management application for monitoring and configuring network devices, including the ACE.

ACE Troubleshooting Wiki

The ACE documentation set now includes the ACE Troubleshooting Wiki. This wiki is a collaborative site that describes the basic procedures and methodology to assist you in troubleshooting the most common problems that you may encounter while you are operating your ACE.

As a registered user of Cisco.com, we strongly encourage you to add content to this site in the form of troubleshooting tips, procedures, or even entire sections. When you add content to the site, you should adhere to the format that has been established for the wiki. To access the Troubleshooting Wiki on Cisco DocWiki, click the following URL:

http://docwiki.cisco.com/wiki/Cisco_Application_Control_Engine_%28ACE%29_Troubleshooting_Guide

Software Version A5(1.2) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(1.2):

Note Some caveats may have more than one number. A number in parentheses is a caveat number that was associated with the previous software release that now has another number for A4(2.0) and later releases.

Software Version A5(1.2) Resolved Caveats

The following resolved caveats apply to software version A5(1.2):

- **CSCsz08381**—When a nontypical Layer 4 type packet is fragmented and the ACE reassembles it, the first 4 bytes of the Layer 4 header on the reassembled packet become corrupted. Workaround: To avoid reassembly, do not fragment the packet.
- **CSCte79279**—When you display the statistics for a policy map using the **show service-policy summary** command, you may see "N/A" in the command output. For example:

```
host1/Admin# show service-policy L4-policy summary
cMap-Any                        17.1.1.10       any   any
OUT-SRVC
N/A
```

  Workaround: None.
- **CSCtg80762**—When you use a management tool for ACE XML formatting using a script, the ACE may add four extra lines to the XML output. You can see the extra lines when you enter the **show service-policy detail** command. The failure is specific to the context where you have performed the formatting. Workaround: Divide the policy map where the VIP is configured.
- **CSCtg87855** (**CSCtg22592**)—After you make a change to a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the **show** command.
- **CSCti85313**—When using the **sticky-serverfarm** command to specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, if a server farm goes down, the ACE fails to display the following system message:

```
%ACE-5-441003: Serverfarm (name) failed in policy_map (policy_name) --> class_map
(cmap_name) without backup. Number of failovers = count1, number of times back in
service = count2
```

  Workaround: None.

- **CSCtj01818**— When the ACE performs a configuration rollback for a configuration that contains a large number of ACLs, the ACE may display the following system error message:

  ```
  %ACE-3-440003: Deletion failed for RedInfoTable.
  ```

  This behavior can occur when you specify the **no associate context** or **no ft group** commands. Workaround: None.

- **CSCtj12692**—You configure the ACE with 4000 sticky groups and do not allocate a sticky resource class. The sticky resource values are the default: minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries, you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context. After a few minutes the ACE becomes unresponsive and reboots. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.

- **CSCtj19992—**While performing a backup for the licenses on the ACE module, the **copy licenses** command fails. Workaround: None.

- **CSCtk94447**—When you enable AAA authentication and remote accounting for TACACS on the ACE and perform the following, the ACE reboots:

  a. Verify the creation of a user by using the **show users** and **show user-account** commands.

  b. Verify AAA accounting.

  c. Enter the **no username** *name* command.

  Workaround: None.

- **CSCtl45638**—When you configure usernames with the ACE default roles, a user with the Network-Monitor role does not have access to some commands. Workaround: Assign the user with the admin role.

- **CSCtl68891**—When you configure a real server on the ACE, assign it an IP address, place it in service, and then delete it, the ACE generates an unnecessary trap. When the real server state changes from ARP-FAILED to operational, the ACE generates the CesRServerStateUp trap. Workaround: None.

- **CSCtn25383**—When you configure a server farm with a scripted probe for health monitoring and scripted probes fail, the ACE does not generate level 3 health probe failed error messages. If you configure SNMP traps, the SNMP device logs the probe failures but the ACE does not generate them in the system log. The expected level 3 message is similar to the following:

  ```
  %ACE-3-251015 Scripted probe failed for server ip_address, error message.
  ```

  Workaround: None.

- **CSCtn31362**—When the remote AAA server is configured in multiple contexts and XML requests through HTTP are sent to multiple contexts, occasionally, the ACE reboots when the AAA daemon becomes unresponsive. For this configuration, the structure for the session is getting freed. After freeing, the session.vcid element is used for printing, causing the AAA daemon to become unresponsive. Also, the other local variable is used for printing. Workaround: None.

- **CSCtn96103**— When the following **banner motd** configurations trigger a config-sync error, the standby ACE transitions to the FSM_FT_STATE_STANDBY_COLD state with a command parse error:

  – h(H)ostname and a space character:

  ```
  switch/Admin(config)# banner motd #
  Enter TEXT message. End with the character '#'.
  > hostname <--------------<SPACE>
  ```

  – h(H)ostname, a space character, and any character:

```
switch/Admin(config)# banner motd #
Enter TEXT message. End with the character '#'.
> hostname a
```

Workaround: Add a colon (:) after the h(H)ostname, for example:

- > hostname: <----------<SPACE>
- > hostname: a

- **CSCto81777**—When you use the CLI to configure a probe on the ACE, you cannot remove the **open** statement. You may also find that even if you did not configure values for probe interval, passdetect interval, and open timeout, those values appear in the ACE running configuration. Workaround: None.
- **CSCto94539**—When you configure probes on the ACE, they unexpectedly stop working and an out of socket condition is reported. An additional syslog is provided to further troubleshoot this type of issue. Workaround: Take the probe out of service and place it back in service. If this action does not resolve the issue, remove the probe from the configuration and reconfigure it.
- **CSCtq24092**—When the ACE imports PEM-encoded SSL certificates or keys with lines that wrap over 70 characters through a terminal, the ACE fails to install the certificate or key. Workaround: Import the certificate remotely through FTP or TFTP.
- **CSCtq38048**—If you find that a restore fails due to an error (for example, if you have nonexportable keys that are missing in the backup), the restore process halts and none of the remaining contexts are restored. This behavior typically occurs during restore due to nonexportable keys missing in the backup. Workaround: None.
- **CSCtq40340**—A half-opened connection (ESTAB/CLOSED) is created on the ACE. Upon receiving a SYN, the ACE sometimes fails to respond with the ACK for the SYN and silently drops the SYN. Without the ACK, the client continues to resend a SYN and the existing entry is never purged until the connection inactivity timer reaches the timeout for idle TCP connections. Workaround: None.
- **CSCtq53880**—The ACE module suddenly reboots due to a watchdog timeout in the kernel. The watchdog timeout also results in a kernel crash information file to be written to the core directory. Workaround: Use the **no system watchdog** command to disable the watchdog.
- **CSCtq64174**—After performing a reload of the ACE, you may find that the **no arp learned-mode enable** command is not shown in the **show running-config** command output. The **arp learned-mode enable** command is an ACE default, so it is shown in the running-configuration file only when the command is disabled; the **show running-config** command output displays “no arp learned-mode.” When an ACE reload occurs, this configuration is copied to the startup-config file. After an ACE reload when the startup-config file is applied to the ACE, the **no arp learned-mode** command generates an error because it is an incomplete command. Workaround: Specify the **no arp learned-mode enable** command in configuration mode, and then specify the **show running-config** command. The **no arp learned-mode enable** command should now appear in the **show running-config** command output.
- **CSCtq67444**—You may find that the ACE is reset by the Catalyst 6500 series switch supervisor engine. In this configuration, you have an SSO setup in the switch with the ACE module, and you perform an SSO switchover. Workaround: None.
- **CSCtq70223**—The ACE sends TACACS+ accounting information in two lines making it slightly more difficult to use the | grep operator. The | grep operator filters CLI command output to display only the output containing the lines of text that match the specified text.

  In the example shown below, “cmd=” is the start of the new line.

```
Mon May 23 11:49:26
```

```
2011 mnl-1slb-01 jwacase 3000 unknown stop task_id=/dev/pts/0_1306171095 stop_time=Mon
May 23 17:49:26 2011
    cmd=0:show runn service=none
```

Workaround: None.

- **CSCtq73968**—In a redundant configuration, the active and standby ACEs display policy map statements in reverse order. For example:

  Active ACE:

```
policy-map type loadbalance first-match ERP-HCMTSTVIP-POLICY
  class class-default
    sticky-serverfarm NEW
    insert-http WL-Proxy-SSL header-value "true"
    insert-http WL-Proxy-Client-IP header-value "%is"
```

  Standby ACE:

```
policy-map type loadbalance first-match ERP-HCMTSTVIP-POLICY
  class class-default
    sticky-serverfarm NEW
    insert-http WL-Proxy-Client-IP header-value "%is"
    insert-http WL-Proxy-SSL header-value "true"
```

  Workaround: None.

- **CSCtq80722**—When you configure a real server in service and have it remain inactive until the primary real server fails (the **inservice standby** command), the ACE config manager may become unresponsive and the ACE reboots. The following system messages may appear:

```
%ACE-2-443001: System experienced fatal failure.Service name:cfgmgr(x) has terminated
on receiving signal 8,system will not be reloaded
%ACE-2-443001:System experienced fatal failure.Service name:cfgmgr(x) crashed, last
core saved,system will not be reloaded
%ACE-2-199006: Orderly reload started at xxx by System. Reload reason: Service
"cfgmgr"
```

  This issue can occur when you use the leastconns, least-loaded, or response predictor to define how the ACE selects a real server in a server farm to service a client request. Workaround: Use the roundrobin predictor for the affected server farm.

- **CSCtr14599**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not being removed completely from the Catalyst 6500 series switch or Cisco 7600 series router. When this behavior occurs, debugging starts on the Catalyst with the message “Failed to remove route.” Workaround: None.

- **CSCtr24875**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not injected in the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior happens when your configuration includes more than 70 VIPs. You will not encounter this issue with an IPv4 address. Workaround: None.

- **CSCtr33704**—In some instances, old routes are not properly removed from the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior can occur under changes that are related to route health injection (RHI). For example:

  – When you configure a global IPv6 address on an interface and the ACE performs duplicate address detection (DAD) for the alias IP address. In this case, the ACE injects a route that corresponds to an interface IP address. Once it passes, the ACE removes the interface and injects a route that corresponds to the alias. This route is not updated properly in the supervisor module.

  - When you configure the ACE to advertise an ACE module VLAN for route health injection (RHI) that is different from the VIP interface VLAN, and you remove the advertised VLAN, the ACE contains the two routes.
  - In a redundant configuration, after a switchover, routes that correspond to the older ACE module are not removed.

  Workaround: Reboot the ACE module.

- **CSCtr34553**—When you remotely access the ACE module CLI through an SSH session, the Last Login: fields appear. These additional fields are not applicable to the ACE30 module and can cause the external scripts to encounter issues when logging into the ACE. Workaround: None.
- **CSCtr31749—**With the ACE configured for **no normalization** on an interface and IP sticky, when the ACE receives packets such as TCP Resets, the connections and sticky entries that are created can cause high CPU conditions. Workaround: Perform one of the following actions to resolve this issue:
  - Specify **normalization** on the interface (unless you are using DSR to provide protection against Distributed Denial of Service (DDoS) attacks on an interface).
  - Remove sticky from the configuration.
- **CSCtr44432**—During normal operation, the ACE module periodically reboots. The ACE reboot results in a kernel crash information file to be written to the core directory, indicating that the system is out of memory. After the ACE reboots, the ACE clears the condition that caused the reboot. Workaround: None.
- **CSCtr49115**—The ACE reboots when you enter the **vsh -c terminal length 0** command and the core directory creates core files similar to the following examples:

```
750330  Jul 11 14:06:45 2011 0x801_vsh_log.16870.tar.gz
750335  Jul 11 14:06:45 2011 0x801_vsh_log.16871.tar.gz
750336  Jul 11 14:06:45 2011 0x801_vsh_log.16879.tar.gz
```

  This behavior may be due to the ACE running out of memory when you execute the **vsh** command. Workaround: None.

- **CSCtr62421**—The ACE may become unresponsive and reboot due to low system memory issues. Workaround: None.
- **CSCtr62530**—When a NAT pool is applied and then removed from a VLAN interface, these actions corrupt the Route table in the ACE. This issue happens when the same NAT pool is applied to multiple VLAN interfaces, and that NAT pool is removed from the first VLAN interface while it is still applied on the second VLAN interface. Workaround: None.
- **CSCtr83034**—In a redundant configuration, after you specify the **no inservice** command followed by the **inservice** command for a real server in a server farm, both ACEs become unresponsive and then reboot. Workaround: None.
- **CSCtr93395**—When UDP Booster is enabled on the ACE to load balance DNS traffic, the source IP address does not appear in the **show conn** command output.

```
host1/Admin# show conn
conn-id    np dir proto vlan source               destination           state
----------+--+---+-----+----+--------------------+---------------------+-----
101646    1  in  UDP   302  0.0.38.114:0         80.58.61.250:53       -
```

  Workaround: None.

- **CSCtr94589**—In a redundant configuration, where contexts are active on both the active and standby ACEs with connection replication and implicit PAT, you may find that TCP port numbers are being reused too quickly. When this issue occurs, the next TCP port number can become corrupted. Workaround: Make all contexts active only on the active ACE.

- **CSCtr96229**—When you remove a resource class that is associated with a specific context, the ACE may reboot. This issue is related to the number of contexts in the ACE when the ACE is configured with several contexts and when a resource class that is associated with one of the contexts requires a sticky limit. When the ACE LB module attempts to remove the sticky entries from the free list, it first determines if there is a starving context that is waiting for resources by walking through a link list of contexts, which consumes the ACE CPU time. This behavior does not occur if the resource class does not include any limits for sticky.

  Workaround: We recommend that you do not change the resource class when there is a large number of contexts or sticky groups configured in the ACE, or that you gradually change the limit in the resource class if you have configured a sticky limit.

- **CSCts00376**—While you attempt to copy a running-configuration file to the ACE from a remote server using TFTP, the ACE displays a "cmd exec error" on the console. The ACE should display an error message when there is a failure in applying the running-configuration file. Workaround: None.

- **CSCts08972**—Control Plane (CP) management access stops when the Configuration Manager (CFGMGR) becames unresponsive while the ACE attempts to compile the regex expression contained in the following command:

  ```
  ssl url rewrite location ^gdsp[\].* sslport 443 clearport 80
  ```

  Similar issues can occur because the CFGMGR consumes a large portion of the CP CPU when compiling certain regex expressions. Workaround: Reboot the ACE and use the alternate regex expression:

  ```
  ssl url rewrite location ^gdsp\.* sslport 443 clearport 80
  ```

- **CSCts14335**—In a redundant configuration, entering the **np session disable** debug command puts the active ACE into the STANDBY_COLD state. Workaround: This debug command is intended only for internal debugging. Do not use the **np session disable** debug command.

- **CSCts24977**—The service name:snmpd(1395) terminates upon receiving signal 8. This issue can occur when polling the ACE CPU utility MIB in a loop; the snmpd process can become unresponsive and cause the ACE to reload. For this particular issue, the OID polled was .1.3.6.1.4.1.9.9.480.1.1.7.1. Workaround: Do not poll the ACE CPU utility MIB continuously in a loop.

- **CSCts29208**—With one or more sticky groups and failaction reassign configured under one of the server farms, the ACE may experience the load balance issue while incrementing real server connection counts. Workaround: When this behavior occurs, do not configure the **failaction reassign** command with the server farm.

- **CSCts30483**— The ACE unexpectedly reboots. If you specify the **show version** command, the reason of the last reboot is due to the watchdog timer in the ACE:

  ```
  last boot reason: Sibyte watchdog reload, kernel space hang
  ```

  Workaround: Use the **no system watchdog** command to disable the watchdog.

- **CSCts41389**—A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server. Multiple Cisco products could be affected by this vulnerability.

  Mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this Advisory:

  http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=24024

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110830-apache.shtml.

PSIRT Evaluation:

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.0/3.3:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C

CVE ID CVE-2011-0956 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCts53405**—After forwarding the real server's first response packet to the client, the ACE waits for the client to send an ACK to the first response packet before forwarding subsequent server response packets. Workaround: Use the **set tcp wan-optimization rtt** command to allow you to control how the ACE applies TCP optimizations to packets on a connection associated with a Layer 7 policy map.
- **CSCts58029**—In a redundant configuration, if a context has “priority” as part of its name, this causes the Admin context to go to STANDBY COLD state. The issue is encountered only during a bulk synchronization. Workaround: Delete any context that includes “priority” in its name and rebuild it with a new name.
- **CSCts68281**—When using a custom configured HTTPS health probe on the ACE, you may encounter the following error message:

  ```
  %ACE-3-400001: MSS mismatch from 10.0.5.193:443 (1380) to 127.1.2.34:64571 (1460) on
  interface vlan40
  ```

  Workaround: The only thing that will stop the errors is to un-apply the Remove the custom HTTPS probe from the server farm to stop the error condition.
- **CSCts69941**—With a large configuration containing a large number of contexts, interfaces, and ACLs (including a merge of individual ACLs into one large ACL), the ACE can become unresponsive 10 to 15 minutes after booting. Workaround: Specify the **show np 1 access-list resource** command after you boot the ACE. Confirm if the Leaf Parameter nodes exceeds 400K and the policy action nodes exceeds 200K (recommended values are 200K and 100K, respectively). If one of these nodes exceeds the specified value, remove the merged ACLs and associated contexts until this threshold is not exceeded in the **show np 1 access-list resource** command output.
- **CSCts79939**—The following rewrite configuration does not successfully rewrite any instances of “http” under some scenarios:

  ```
  action-list type modify http REWRITE
    header rewrite response Location header-value "(.*)http(.*)" replace "%1https%2"
  ```

  While parsing the Location header, the ACE stops parsing after encountering any instance of the first letter in the match string (“h”). At that point, the ACE does not complete the match or perform the rewrite. Workaround: None.
- **CSCts98720**—In an application where the ACE is performing firewall load-balancing with two server farms (where one server farm is for user traffic and the one is for BGP traffic sent to the firewalls), when the ACE performs a failaction reassign and then undoing the failaction, the ACE incorrectly moves a user connection to the BGP dedicated server farm. Workaround: None.

- **CSCtt02508**—An end-to-end SSL TCP connection encounters issues while uploading a large (approximately 4.5 GB) file through an ACE VIP that is configured for end-to-end SSL. Simultaneous front and back-end traces show that the ACE brings the TCP window to zero on the client side but does not send any further data toward the server on the back-end side even though the last TCP window update from the server is 65K. The upload stops and never resumes after that. Note that this issue is not seen with a Layer 4 server load-balancing VIP configuration. Workaround: None.
- **CSCtt14768**— The ACE may start dropping connections due to an unavailable buffer. This issue is related to improper handling of an HTTP GET request to the ACE VIP. The issue is verified only if you enable Layer 7 application inspection. You will notice the connection buffer utilization is slowly increasing. Workaround: Clear the connection to clear all stale connections and to release the buffer.

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.0/3.3:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C

  CVE ID CVE-2011-0956 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
- **CSCtt24046**—When the ACE performs multiple simultaneous SNMP requests on the cpmProcessTable, this may result in an SNMP timeout. Workaround: Perform only sequential SNMP requests on Cisco Process MIB.
- **CSCtt42497**—When performing Layer 7 server load balancing with a configuration that includes a combination of sticky, server connection reuse, and persistence-rebalance, bad HTTP requests may occur on the server as Layer 7 HTTP packets are sent out of order. Packets sent out of order cause the server to drop the packets or tag the request as malformed. Workaround: Disable the server-conn reuse command.
- **CSCtt47587**—HTTPS probes fail only for IIS servers with client certificates mode “Accept client certificates.” In this case, IIS servers with “ignore client certificates” are not impacted. Workaround: Perform one of the following actions:
  - Configure the IIS server to “ignore client certificates.”
  - Configure a TCP probe instead of an HTTPS probe.
- **CSCtt76277**—In a redundant configuration, the standby ACE module is in an active state when it is reloaded from the Catalyst supervisor engine through the **no power enable** or **hw module reset** command. Workaround: Perform one of the following actions:
  - Create the file “skip_reset_cde_hash_table” by specifying the following command sequence on the Catalyst supervisor engine:

    ```
    show clock > disk0:skip_reset_cde_hash_table
    ```

Note When the fix is out, be sure to delete the file with the **del disk0:skip_reset_cde_hash_table** command.

  - Configure an input ACL on the ACE VLAN interfaces to deny multicast traffic. For example, enter:

    ```
    access-list deny_mcast line 10 extended deny ip any 224.0.0.0 240.0.0.0
    ```

```
access-list deny_mcast line 20 extended permit icmp any any
access-list deny_mcast line 30 extended permit ip any any
```

- **CSCtu10624**—Establishing a Telnet connection from the ACE to a remote device is silent with no indication of a successful connection or DNS resolution. When this issue occurs, the lines “trying...” and “connected...” are not seen. Workaround: None.
- **CSCtu01626**—The HTTP probe with a regex search string fails when the HTTP header is split into two packets. When this issue occurs, HTTP probes pass and fail intermittently. Workaround: The server needs to send the entire header in one receive packet and not split the header into two packets.
- **CSCtu03063**—The ACE appliance may encounter leaking 64k buffers on the NP which, when it reaches above 75%, stops passing traffic. This behavior occurs whenever a UDP port 69 probe succeeds. Note that when the probe fails, the buffer does not leak.

  An example of the **show np buffer usage** command is as follows:

  ```
  ACE/Admin# show np 1 buffer usage
  Total Internal Buffer    : 155648
  Internal Buffer Used     : 145139
  Percentage of Buffer Used: 93.25%
  Automatic reload         : disabled
  ```

  This system message appears when this condition occurs:

  ```
  ACE %ACE-3-443004:Available NP 1 buffer reached below 12 percent threshold, Total
  buffer:155648, Available Buffer:11694
  ```

  Workaround: To set threshold levels for the NP buffers in the active and the standby ACEs and cause the active ACE to reboot if the thresholds are reached or exceeded, use the **buffer threshold** command.
- **CSCtu27310—** With the ACE configured in bridge mode, a DHCP client on a VLAN located behind the ACE, is unable to obtain a lease from a DHCP server located in front of the ACE. This behavior happens only with a Linux-based DHCP server. Workaround: Use a different DHCP server with a broadcast reply (not a unicast reply).
- **CSCtu30517—** With switch-mode enabled on a shared interface with SYN-cookie-based DoS protection configured, embryonic connections are not counted properly in the **show syn-cookie** output. Workaround: None.
- **CSCtu33882**—During normal operation of the ACE through a remote SSH connection, the remote SSH connection suddenly starts to fail. The ACE requires an indication through a counter or syslog to indicate what is preventing SSH from working. Workaround: None.
- **CSCtu34037**— User context configurations (including certificates and keys) are lost after the ACE reloads. When this issue occurs, the Admin context configuration is reduced to the minimal, initial configuration. This issue can occur when you specify the **reload** command, or if the FT link is interrupted by high CPU usage on the switch that the ACE is connected to. Workaround: None.
- **CSCtu34163**—You attempt to establish a remote SSH connection to the ACE and the ACE reboots and then generates a SSHD core file. Workaround: None.
- **CSCtu36146**—The ACE becomes unresponsive due to a configuration manager (Cfgmgr) process failure with the last boot reason: Service “cfgmgr.”

The following example system error log messages may appear shortly before the ACE reloads:

```
MG6509:7:Admin 443001 Critical 24-Oct-2011 08:29:09 System experienced fatal
failure.Service name:cfgmgr(1050) has terminated on receiving signal 11,system will
not be reloaded

MG6509:7:Admin 443001 Critical 24-Oct-2011 08:30:23 System experienced fatal
failure.Service name:cfgmgr(1050) crashed, last core saved,system will not be reloaded

MG6509:7:Admin 199006 Critical 24-Oct-2011 08:30:31 Orderly reload started at Mon Oct
24 13:30:28 2011 by System. Reload reason: Service "cfgmgr"
```

Workaround: None.

- **CSCtv12765 (CSCtx25605)**—When you have a Layer 7 class map that includes multiple access-list matches, the ACE may send resets to a VIP that has multiple Layer 7 matches. Workaround: Remove the ACL class map(s) from your ACE configuration.
- **CSCtv17196**—The **show script code** command returns an invalid call. Workaround: Reboot the ACE.
- **CSCtw46194—**RHI routes fail to be removed from the Catalyst supervisor engine when you remove a VIP from a Layer 3 class map. Workaround: None.
- **CSCtw53737—**When using an outbound access-group on a VLAN interface, traffic that is is explicitly permitted in the configuration may be dropped. HTTPS probes may also become unresponsive for specific real servers while TCP probes continue to work. When this behavior occurs, the following example system message may appear:

  ```
  %ACE-4-106023: Deny tcp src vlanxxxx xxx.xxx.xxx.xxx/xxxxx dst
  undetermined:xxx.xxx.xxx.xxx/xxxx by access-group "<name>" [0xffffffff, 0x0]
  ```

  Workaround: Use an inbound access-group on the VLAN interface.
- **CSCtw70955**—The ACE strips the checksum when you enable **inspect dns** to perform DNS application protocol inspection. There is no additional impact to DNS application protocol inspection. Workaround: None.
- **CSCtw76940**—You may find that double quotations in a description are replaced by spaces. For example, if you configure **description t"e"st**, this description is displayed as `description t e st` in the **show running configuration** command output as follows:

  ```
  (config-if)# description t"e"st
  (config-if)# do sh run | i desc
  Generating configuration....
    description t e st
  ```

  You may encounter this behavior when strings between double quotations do not include a space. This **show** output display issue does not occur if you insert a space between the double quotations (for example, **description t" e"st**). In this case, a space is inserted between " and e. For example:

  ```
  (config-if)# description t" e"st
  (config-if)# do sh run | i desc
  Generating configuration....
    description t " e" st
  ```

  Workaround: None.
- **CSCtw84303**—The ACE downloads the CRL for the first time from the specified CRL download location. However, subsequent updates are not attempted after the ACE NextUpdate timer expires. Workaround: None.

Software Version A5(1.2) Open Caveats

The following open caveats apply to software version A5(1.2):

- **CSCtd42287**—When the ACE is running with the maximum limit of 8 K static entries and you remove a service policy from an interface and quickly re-add it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then re-adding it.
- **CSCte76618**—When traffic traverses the ACE module with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCtf54230**—When Layer 2-connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate of traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.
- **CSCth16258**—The **snmpwalk** or **bulkwalk** command on the SSL proxy MIB always returns a timeout. Currently, there is no tnrpc call to fetch data. The number of statistics has increased to string parsing and is taking more time. The default timeout is one second and it is not responding within one second. Workaround: Increase the timeout value.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

  Workaround: Remove and reconfigure the real server.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

  ```
  System running low on direct mapped memory
  Please issue 'show system kcache' to diagnose further
  ```

  Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.
- **CSCtj30825**—When you configure a large number of ICMP probes and directly connected hosts on the ACE, ARP resolution fails intermittently for the directly connected hosts. Workaround: Decrease the number of ICMP probes or change the ICMP probes to TCP or UDP-based probes.
- **CSCtj60979**—The ACE suddenly reloads with the reason identified as “me-dumper crash.” In rare cases, the **show np 1 me-stats** command causes the me-dumper crash. Workaround: None.
- **CSCtj65628**—When you configure RBAC on an ACE with a custom role and domain, any permit rule allows all **show** commands to be entered regardless of the configured permissions. Workaround: None.
- **CSCtj65634**—When the maximum aclmerge instance limit of 8191 is reached and then freed, ACL merge will not occur. Also, after reaching the maximum limit of instances, if you remove the outbound ACL from the interface, the policy action nodes are not released. Workaround: None.
- **CSCtl54305**—When HTTP, DNS, and SIP inspection load balancing and no contexts are active on a standby ACE and the supervisor is running s72033-adventerprisek9_wan_dbg-mz.SIERRA_INTEG_101111, the supervisor logs an ACE observed storm control message, similar to the following:

```
%PM_PLATFORM-5-PORTDROP: Port TenGigabitEthernet3/1 dropped packets due to storm
control
```

The message had no impact on operations. Workaround: None.

- **CSCto76442**—When you configure a new IPv6 duplicate address attempt for an interface through the **ipv6 nd dad-attempts** command, you may find that the value does not take effect. Workaround: Specify a shut/no shut command sequence on the interface to reenable the interface. We recommend that prior to specifying a shut/no shut command sequence that you keep track of the current traffic movement on the interface.
- **CSCtr09972—**SNMP queries are incomplete with the error "snmpwalk: Unknown user name." This behavior is encountered when doing an snmp walk on the following object identifier (OID) cpmProcessExtRevTable on two contexts simultaneously. Workaround: None.
- **CSCtr56096**—You may observe that the sticky-conns counter in the **show serverfarm detail** command output displays a nonzero value when there are no current connections. The sticky-conns counter displays the number of active connections when using sticky and gets updated when there are one or more active (current) connections. Workaround: None.
- **CSCtr58692**—You may find that configuring the **fail-on-all** command, followed by a probe, for a real server does not function properly. Workaround: After adding or removing a probe for a real server, remove and re-add the **fail-on-all** command for the real server.
- **CSCtr79276**— The ACE does not work properly in one-arm mode with SIP and TCP when source NAT is enabled. SIP registrations and calls may fail depending on whether SIP Inspect is enabled. Workaround: None.
- **CSCtr80967**—With SIP traffic running for a long period of time (for example, overnight) with a heavy volume of traffic, the ACE may encounter a few proxy map entries that leak. For example:

```
switch/Admin# sh np 1 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32767             0
Alloc Proxy Mapping:                       29612485            0
Alloc Proxy Mapping Failed:                       0            0
Release Proxy Mapping:                     29612484            0
switch/Admin# sh np 2 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32768             0
Alloc Proxy Mapping:                       33107573            0
Alloc Proxy Mapping Failed:                       0            0
Release Proxy Mapping:                     33107573            0
switch/Admin# sh np 3 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32766             0
Alloc Proxy Mapping:                       50967736            0
Alloc Proxy Mapping Failed:                       0            0
Release Proxy Mapping:                     50967734            0
switch/Admin# sh np 4 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32766             0
Alloc Proxy Mapping:                       52207388            0
Alloc Proxy Mapping Failed:                       0            0
Release Proxy Mapping:                     52207386            0

switch/Admin# sh np 1 me-stats "-D"
0 entries open.
```

Workaround: None.

- **CSCtr81263**—With high point-to-multipoint traffic, the ACE may ignore the specified connection limit specified by the **conn-limit max** command. In this case, you may observe few connections being received over the configured connection limit. Workaround: None.

- **CSCtr94921**—When you configure the ACE with SIP inspection and load balancing, under heavy traffic some of the network processors may run out of buffers. When this occurs, the ACE intermittently drops traffic across all contexts. Workaround: None.
- **CSCts09006**—Under normal operations with SNMP, the ACE unexpectedly reloads and generates a core file. Workaround: None.
- **CSCts25057**—Connections to a real server may not be purged with the **failaction-purge** command, and the real server enters a return code failed state. Workaround: None.
- **CSCts36540**—In a redundant configuration, with multi-context sticky traffic, if you perform an FT switchover while under heavy traffic and the sticky database is full, the ACE will reboot. Workaround: Increase the sticky timeout value.
- **CSCts40787**—In a redundant configuration, multiple (repeated) flaps on the Catalyst supervisor engine on the FT VLAN causes the configuration controller process in the ACE to become unresponsive and the ACE reboots. Workaround: None.
- **CSCts42706**—When performing IPv6 processing, you may find that Bridge Protocol Data Units (BPDUs) are dropped by the ACE and do not get bridged. Workaround: Perform one of the following actions to resolve this issue:
  - Configure an IPv4 address.
  - Remove and then add the **ipv6 enable** command under the interface to enable IPv6 processing on the interface.
- **CSCts47978**—The ACE module may incorrectly use a custom TCL script for SSL probes with the -sslversion option. For example:

  ```
  set sock [socket -sslversion version -sslcipher cipher $ip $port]
  ```

  When this issue occurs, the following error messages can be seen in the **show script** <*script file name*> <*probe name*> command output:

  ```
  Internal error     = bad option "-sslversion": must be -async, -myaddr, -myport, or
  -server
  ```

  Workaround: Use a different keepalive type.
- **CSCts50072**—When running an ACE module for over 100 days under normal conditions but with a large configuration, the ACE warns of low memory. Workaround: Reduce the size of the configuration. Reboot the ACE when the memory falls below one percent.
- **CSCts56552—**In a P2MP scenario, there are multiple SIP connections between a client and server, and the connection is terminated with BYE. In this case, the BYE should clean the entries for the connection in the ACE, or the table will get full and a RESET would be issued to close the SIP session. Workaround: None.
- **CSCts60292**—After enabling SYN-cookie-based DoS protection for an interface, when the SYN-cookie limit is reached and when a post request is sent, the request fails. In this case, the first segment reaches the server and subsequent segments get lost. Workaround: None.
- **CSCts67012**—When operating in a redundant configuration, you may observe a kernel crash on the standby ACE when receiving both IPv4 and IPv6 traffic. In this case, both real servers and clients cause intermittent reachability issues due to IPv6 Neighbor Discovery (ND) failures. Workaround: Configure your IPv6 clients to be one hop away from the ACE.
- **CSCtt23176—**You are using an ICMP probe attached to a transparent server farm, and the probe stops sending an ICMP echo request after about 12 hours of continuos operation. Workaround: Use a UDP or TCP probe.

- **CSCtt33804**—During modification of an access control list (ACL) within a context, an ACL merge error may be reported on one or more of the interfaces where the ACL list is applied, leaving the interface in an inconsistent state. When this issue occurs the following system message appears:

```
%ACE-1-106028: WARNING: ACL Merge failed to locate specified ACL in context 10049.
Error while processing service-policy. Incomplete rule is currently applied on
interface vlan200. Configuration on this interface needs to be manually reverted
```

Workaround: Perform one of the following actions:

- Remove the offending lines one at a time from the ACL until the ACL can be successfully applied.
- Reload the ACE.

- **CSCtt61028**—When operating in a redundant configuration, SSL probes fail intermittently even if the ACE module is in standby mode. Workaround: Reload the ACE.
- **CSCtu18281**—The restore process may fail if the Admin context in the backup configuration has TACACS authorization and the configuration is associated with a domain (**add-object** command). When this issue occurs, the restore process fails and the non-Admin contexts are not imported. However, for the Admin context, the configurations are properly applied. Workaround: Remove "domain TACACS" from the backup configuration and perform the restore.
- **CSCtu33484**—When setting the idle timeout on the ACE, an extra second is added for every minute of idle time. When this issue occurs, the connection disappears from the statistics on the configured time. The reset is not sent until the idle time plus the extra time expires. Workaround: None.
- **CSCtw37578**—In a redundant configuration, if you add or delete an SNMP user and then perform an SNMP MIB walk, these actions can result in the service name:snmpd(1395) becoming nonresponsive and the ACE rebooting. You may then see a similar system message error on the ACE:

```
Dec 18 2011 20:35:54 :%ACE-2-443001: System experienced fatal failure.Service
name:snmpd(1035) has terminated on receiving signal 11,system will not be reloaded

Service name:snmpd(1035) has terminated on receiving signal 11
```

  Workaround: None.

- **CSCtw58766—**With SIP load balancing configured without Layer 7 SIP inspection, when the client sends a SIP INVITE message as two segments, the second packet is dropped by the ACE. This issue can also occur when two consecutive SIP calls make it through the same control connection and the INVITE message is segmented so that only the body is contained in the second segment. Workaround: Configure a Layer 7 SIP inspection policy.
- **CSCtw64351—**A soft lockup occurs on CPU#0 after you specify the **show np 1 lb-stats** command. Workaround: None.
- **CSCtw68905**—OSPFv3 neighborship does not work with the ACE module configured in bridge mode. Workaround: None.
- **CSCtw79419**—An error occurs when you attempt to delete a server farm, and the ACE prevents you from performing the deletion. This behavior can occur when the ACE configuration manager still associates the server farm with a load balancing policy. For example:

```
ACE/1(config)# no serverfarm host 2081bancaPR
Error: serverfarm 'SERVERFARM_X' is in use. Cannot delete!
```

  Workaround: Reboot the ACE.

- **CSCtw80406**—In a redundant configuration, the standby ACE may become unresponsive and reboot after operating for more than five hours. This behavior typically occurs when you perform SNMP polling and an SNMP walk at the same time in multiple terminals with a heavy redundancy configuration, while creating and killing an SSH session multiple times. Workaround: None.
- **CSCtu80983**—With a Layer 7 load balancing policy that includes the default class map and HTTP persistence rebalance enabled, when a client sends multiple get requests on the same connection, the hit count in the **show service policy details** command output fails to increment for every GET request. Workaround: None.

- **CSCtw81056—**When performing Layer 7 load balancing with TCP server connection reuse enabled, you may find that intermittent client connections are reset. Traces show a Reset from the backend server occurring immediately after the ACE forwards the client's GET request on the backend. The ACE attempts to reuse a connection on the backend server that was closed on the server. Prior to this failure, the server attempted to close an inactive backend connection, but the ACE ignored and dropped the Fin Ack packets received from the server. Workaround: Reboot the ACE.
- **CSCtx12159**—The ACE becomes unresponsive and reboots, with the last reboot reason of “CP kernel crash.” Workaround: None.

Software Version A5(1.2) Command Changes

Table 5 lists the command changes in software version A5(1.2).

Table 5 CLI Command Changes in Version A5(1.2)

Mode	Command and Syntax	Description
Exec	**show connections**	Per CSCtr93395, when you configure the UDP booster feature using the **udp** command, it displays a hash value for the client address for the **udp ip-source-hash** and u**dp ip-destination-hash** configuration in the **show connections** command output (IPv6 and IPv4 output).
	show service-policy	Per CSCtn73488,the **show service-policy** command now includes the conns per second field that displays the connections per second at the virtual server level when you configure more than one VIP under a class map. When you configure one VIP under a class map, the connections per second field is at the VIP level.

	show service-policy, show server-farm	Per CSCtu21857, a new real server state, DWS-LOCAL-DOWN, has been added to software version A5(1.2) for the dynamic workload scaling (DWS) local feature. This state informs you that a real server is unavailable for load balancing because its locality is remote in a server farm configured for **dws local**.
		
		For example, the **show serverfarm** command displays the DWS-LOCAL-DOWN state as follows:
		
		`Admin(config-sfarm-host)# do show serverfarm sf1`
		
		`Codes: L - local, R - remote`
		
		`serverfarm : sf1, type: HOST`
		`total rservers : 3`
		`state : ACTIVE`
		`DWS state : ENABLED_LOCAL_LB`
		`----------`
		
		`- --------connections----------`
		`real weight state current total failures`
		`--+------+------------+----------+----------+---------`
		`rserver: pod7-vm1`
		`20.1.1.10:0 8 ARP_FAILED [L]0 0 0`
		`rserver: pod7-vm2`
		`20.1.1.11:0 8 OPERATIONAL [L]0 0 0`
		`rserver: pod8-vm1`
		`20.1.1.20:0 8 DWS-LOCAL-DOWN[R] 0 0 0`
		
		For background details on DWS, see Chapter 5, Configuring Dynamic Workload Scaling, in the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Table 5 CLI Command Changes in Version A5(1.2) (continued)

Mode	Command and Syntax	Description

	show service-policy *policy-name* **class-map detail**	Per CSCtu23679, the **show service-policy** *policy-name* **class-map detail** command output includes the Total Logged field under the Layer 7 policy statistic so that the output will be similar to that of Layer 4 policy statistics. For example:
		`L4 policy stats:`
		`  Total Req/Resp: 0, Total Allowed: 0`
		`  Total Dropped: 0, Total Logged: 0`
		`L7 Inspect policy : inspect_http`
		`  class/match : http_insp`
		`  Inspect action:`
		`  permit`
		`  L7 policy stats:`
		`  Total Inspected: 0, Total Matched: 0`
		`  Total Dropped OnError: 0, Total Logged: 0`
		`  Parameter-map(s):`
		`  ECOM_HTTP_PARAM`

Software Version A5(1.2) System Log Messages

Software version A5(1.2) includes the following new system log (syslog) messages and syslog identifier changes.

251015

Error Message `%ACE-3-251015: Scripted probe failed for server IPv4/IPv6 address, error message.`

Explanation Per CSCtn25383, the following Level-3 syslog shown above has been added to identify a scripted probe failure. This system log appears when the configured real server failed its health checks because the associated server response is not as expected or there was an internal error. The possible values of the *error message* variable are as follows:

- Probe error: Server did not respond as expected
- Internal error: Fork failed for TCL script
- Internal error: Script probe terminated due to timeout
- Internal error: TCL interpreter PANIC
- Internal error: Script error
- Internal error: Script-file lookup failed or empty buffer
- Internal error: Failed to allocate memory for tcl workerthread qnode
- Internal error: Unknown script error
- Internal error: Out of sockets for the TCL script
- Internal error: Unable to read persistent variable table
- Internal error: PData (probe data) pointer is null

For example:

```
%ACE-3-251015: Scripted probe failed for server 25.25.25.83, Internal error: Script
error

%ACE-3-251015: Scripted probe failed for server 2021:200::21c:23ff:fee3:a42, Probe
error: Server did not respond as expected
```

Recommended Action Perform one of the following actions:

- Check the service running on the server.
- Check the script used for the probe.
- Check the memory available for TCL scripts.

251021

Error Message `%ACE-4-251021: Health Monitoring connection info invalid, socket:xxxx, socket_state:yyyy, connection_state:zzzz`

Explanation Per CSCto94539, the corruption of health monitoring socket connection information is flagged by this Level 4 syslog. The error message variables are as follows:

- *socket:xxxx* displays a negative value.
- *socket_state:yyyy*, *connection_state:zzzz* displays invalid (mostly large) positive or negative values.

For example:

```
%ACE-4-251021: Health Monitor connection info invalid, socket: 44,
socket_state: 1853121902, connection_state: 9

%ACE-4-251021: Health Monitor connection info invalid, socket: -1428151032,
socket_state: 3, connection_state: 9
```

Recommended Action Check whether health monitoring is functioning properly on the ACE. If there appears to be issues with health monitoring, contact TAC for further troubleshooting.

322006

Error Message `%ACE-3-322006: All xinetd services denied except telnet: Avaliable CP memory(HighMem) reached below 5 percent threshold.`

Explanation Per CSCtu33882, SSH connections may be rejected due to low memory in the ACE. This issue can occur when the available control plane (CP) high memory goes below the five percent threshold.

Recommended Action Check for memory resources by using the **show system kmem** command. The HighFree field in the **show system kmem** command output should be less than 5 percent of the HighTotal value, as shown in the example below. If an SSH connection is causing this low memory condition, use Telnet to establish a remote connection to the ACE. If this problem persists, contact TAC for further troubleshooting.

```
ACE/Admin# show system kmem
MemTotal:      6097528 kB
MemFree:        631164 kB
Buffers:         26000 kB
Cached:        1211600 kB
SwapCached:          0 kB
Active:        4762776 kB
Inactive:       410232 kB
HighTotal:     5373888 kB
HighFree:       220416 kB   <<<<<<<<<<<<<<<  <5% of HighTotal value
LowTotal:       723640 kB
LowFree:        410748 kB
SwapTotal:           0 kB
SwapFree:            0 kB
Dirty:              40 kB
Writeback:           0 kB
Mapped:        4021076 kB
Slab:           211924 kB
CommitLimit:   3048764 kB
Committed_AS: 49686232 kB
PageTables:      51480 kB
VmallocTotal:   114680 kB
VmallocUsed:     69020 kB
VmallocChunk:    45560 kB
```

Software Version A5(1.1) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(1.1):

Note Some caveats may have more than one number. A number in parentheses is a caveat number that was associated with the previous software release that now has another number for A4(2.0) and later releases.

Software Version A5(1.1) Resolved Caveats

The following resolved caveats apply to software version A5(1.1):

- **CSCth46984**—When you assign VLANs to the ACE module in a Cisco Catalyst SUP-2T VSS configuration, error messages flood the supervisor engine console. Workaround: None.
- **CSCth90592**—When you configure static NAT port redirection, the ACE does not apply the configuration and displays the following error message:

  ```
  Error: A static ip and source port must be provided in ACL for static port redirection
  ```

  Workaround: Configure a source port in the ACL for static port redirection.
- **CSCtj65408**—When you configure an ECHO TCP or UDP probe with send-data value, the probe passes even when the server sends a regex that does not match the send-data value. Workaround: You can use a TCP or UDP probe with send-data and regex values as required instead of an ECHO TCP or UDP probe.
- **CSCtk84003**—When you set the window scale to ALLOW by configuring the **tcp-option window-scale allow** command in a parameter map, the window size calculation for the Layer 4 flows does not occur. Because the ACE calculates the window size without taking the window scale into account for Layer 4 flows, the ACE may drop some packets that are legal. Layer 7 flows are not affected. Workaround: Remove the **tcp-option window-scale allow** command from the parameter map configuration.
- **CSCtl53644**—When you configure access lists on the ACE, and if there is an ACL merge error on the internal VLAN4095, you cannot display the error counters through the **show vlan** *number* command because the user-configured VLAN number ends at 4094. Workaround: None.
- **CSCtn57216**—The ACE requires SUP2T support and new firmware. Workaround: None.
- **CSCtn62319**—When the supervisor engine detects that the ACE is not responding to keepalives, the ACE may silently reboot and not generate core dump files. Workaround: None.
- **CSCtn93288**—When redundant ACEs generate SIP probes with the same Call-ID and From-Tag options, the SIP registrar servers interpret these probe messages as duplicates and do not reply to them causing SIP health probes to fail. Workaround: None.

- **CSCto34856**—When you configure Layer 7 load-balancing or HTTPS termination with sticky and redundancy on the ACE, HTTP/HTTPS Post requests with large headers that span multiple packets can cause packets to be sent to the backend servers out of order. This behavior can cause the server to drop the request to or to send a failure return-code. Workaround: Remove sticky from the server farm.
- **CSCto68956**—With the ACE configured for sticky and multiple sticky groups, and the sticky database is almost full, the ACE can unexpectedly reboot and generate a core file. When this behavior occurs, the core file points to the Load Balancing (LB) process thread where a new sticky entry is trying to be obtained. Workaround: None.
- **CSCtq37365**—When a redundancy switchover occurs on the ACE in a VSS setup, the Catalyst 6500 series switch does not receive the purge messages. Workaround: None.
- **CSCts41981**—On rare conditions, after the ACE bootup sequence completes, default license limits are displayed instead of the installed license limits. In this case, if you specify the **show resource usage all** and **show license status** commands, the **show resource usage all** output displays default license values that differ from those displayed in the **show license status** command output. Workaround: Restart the ACE.
- **CSCts56112**—If you have dynamic workload scaling (DWS) configured in the ACE, ACE connectivity with the Cisco Nexus 7000 series switch may be lost. When this happens, SSH connection to the Cisco Nexus 7000 series switch from the ACE reports an "authentication failure" error. Workaround: Perform the following actions:
  - On the newly active Cisco Nexus 7000 series switch, assign a new management IP address.
  - On the ACE, update the IP address of the Nexus 7000 management interface for the local Nexus device on the ACE to the newly assigned IP address.
- **CSCts76353**—In some cases, you may find that real servers frequently reach the INBAND-FAIL state. This issue occurs because the reset interval in the inband health monitoring function is working in seconds instead of milliseconds, which causes the error interval detection to be longer and increases the chance of hitting the INBAND-FAIL state. There are no issues with the other associated real server timers (such as reset, resume-service, and so on); they all appear to be working properly. Workaround: None.
- **CSCts79885**—In a redundant configuration, persistent connections do not properly flow through the ACE after first switchover occurs; only the first request in the persistent connections gets serviced, and the client waits indefinitely for a response to the second request. Workaround: None.
- **CSCtt08368**—You specify the **show tech-support details** command and the resulting size of the output file on the ACE is extremely large. In some cases, the resulting **show tech-support** output file can become so large that the ACE can run out of disk space. Workaround: Individually specify the **show** command output using the individual keywords of the **show tech-support** command. Each command output is separated by the line and the command that precedes the output.

Software Version A5(1.1) Open Caveats

The following open caveats apply to software version A5(1.1):

- **CSCtd42287**—When the ACE is running with the maximum limit of 8 K static entries and you remove a service policy from an interface and quickly re-add it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then re-adding it.

- **CSCte76618**—When traffic traverses the ACE module with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCtf54230**—When Layer 2-connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate of traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.
- **CSCtg87855** (**CSCtg22592**)—After you make a change to a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the **show** command.
- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After the ACE performs the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

  Workaround: Remove and reconfigure the real server.
- **CSCti68449** (**CSCtf43237**)—The **show xlate** command displays thousands of entries. However, the **show resource usage** command displays zero peak and zero current. Workaround: Reboot the ACE.
- **CSCti85064**—Occasionally when the ACE is under high control plane (CP) stress with a high rate of CP syslog traffic at logging Level 7, the CP becomes sluggish. If the data plane becomes unresponsive, the ACE console become unresponsive and the ACE reboots by the SME process without creating any dataplane core files. Workaround: Avoid CP syslogs at level 7 with a high rate of traffic, or enable only fast path syslogs.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

  ```
  System running low on direct mapped memory
  Please issue 'show system kcache' to diagnose further
  ```

  Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.

- **CSCtj12692**—You configure the ACE with 4000 sticky groups and do not allocate a sticky resource class. The sticky resource values are the default: minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries, you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context. After a few minutes the ACE becomes unresponsive and reboots. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj30825**—When you configure a large number of ICMP probes and directly connected hosts on the ACE, ARP resolution fails intermittently for the directly connected hosts. Workaround: Decrease the number of ICMP probes or change the ICMP probes to TCP or UDP-based probes.
- **CSCtj60979**—The ACE suddenly reloads with the reason identified as "me-dumper crash." In rare cases, the **show np 1 me-stats** command causes the me-dumper crash. Workaround: None.
- **CSCtj65628**—When you configure RBAC on an ACE with a custom role and domain, any permit rule allows all **show** commands to be entered regardless of the configured permissions. Workaround: None.
- **CSCtj65634**—When the maximum aclmerge instance limit of 8191 is reached and then freed, ACL merge will not occur. Also, after reaching the maximum limit of instances, if you remove the outbound ACL from the interface, the policy action nodes are not released. Workaround: None.
- **CSCtj65687**—If the VIP address conflicts with the shared interface address across contexts, the standby ACE goes into the cold state with the **show ft config-error** command displaying the following error message:

  ```
  interface vlan number
  Error: Global Policy applied, conflicts with VIP, NAT or Interface IP in shared
  interface!
  ```

  Workaround: Do not configure a VIP address with the same address as the shared interface IP address on which the service policy is configured.
- **CSCtj65693**—The **ip name-server** command is seen in the standby mode even after removing it in active mode. This issue happens in redundant configuration. Workaround: None.
- **CSCtl45638**—When you configure usernames with the ACE default roles, a user with the Network-Monitor role does not have access to some commands. Workaround: Assign the user with the admin role.
- **CSCtl54305**—When HTTP, DNS, and SIP inspection load balancing and no contexts are active on a standby ACE and the supervisor is running s72033-adventerprisek9_wan_dbg-mz.SIERRA_INTEG_101111, the supervisor logs an ACE observed storm control message, similar to the following:

  ```
  %PM_PLATFORM-5-PORTDROP: Port TenGigabitEthernet3/1 dropped packets due to storm
  control
  ```

  The message had no impact on operations. Workaround: None.
- **CSCtl68891**—When you configure a real server on the ACE, assign it an IP address, place it in service, and then delete it, the ACE generates an unnecessary trap. When the real server state changes from ARP-FAILED to operational, the ACE generates the CesRServerStateUp trap. Workaround: None.
- **CSCto76442**—When you configure a new IPv6 duplicate address attempt for an interface through the **ipv6 nd dad-attempts** command, you may find that the value does not take effect. Workaround: Specify a shut/no shut command sequence on the interface to reenable the interface. We recommend that prior to specifying a shut/no shut command sequence that you keep track of the current traffic movement on the interface.

- **CSCtq67444**—You may find that the ACE is reset by the Catalyst 6500 series switch supervisor engine. In this configuration, you have SSO setup in the switch with the ACE module, and you perform an SSO switchover. Workaround: None.
- **CSCtr14599**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not being removed completely from the Catalyst 6500 series switch or Cisco 7600 series router. When this behavior occurs, debugging starts on the Catalyst with the message "Failed to remove route." Workaround: None.
- **CSCtr24875**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not injected in the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior happens when your configuration includes more than 70 VIPs. You will not encounter this issue with an IPv4 address. Workaround: None.
- **CSCtr33704**—In some instances, old routes are not properly removed from the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior can occur under changes that are related to to route health injection (RHI). For example:
  - When you configure a global IPv6 address on an interface and the ACE performs duplicate address detection (DAD) for the alias IP address. In this case, the ACE injects a route that corresponds to an interface IP address. Once it passes, the ACE removes the interface and injects a route that corresponds to the alias. This route is not updated properly in the supervisor module.
  - When you configure the ACE to advertise an ACE module VLAN for route health injection (RHI) that is different from the VIP interface VLAN, and you remove the advertised VLAN, the ACE contains the two routes.
  - In a redundant configuration, after a switchover, routes that correspond to the older ACE module are not removed.

  Workaround: Reboot the ACE module.
- **CSCtr34553**—When you remotely access the ACE module CLI through an SSH session, the Last Login: fields appear. These additional fields are not applicable to the ACE30 module and can cause the external scripts to encounter issues when logging into the ACE. Workaround: None.
- **CSCtr56096**—You may observe that the sticky-conns counter in the **show serverfarm detail** command output displays a nonzero value when there are no current connections. The sticky-conns counter displays the number of active connections when using sticky and gets updated when there are one or more active (current) connections. Workaround: None.
- **CSCtr58692**—You may find that configuring the **fail-on-all** command, followed by a probe, for a real server does not function properly. Workaround: After adding or removing a probe for a real server, remove and re-add the **fail-on-all** command for the real server.
- **CSCtr70477**—You may observe that the **show service policy detail** command output includes invalid values for the Hit Count or Dropped Conns counters under the class-default class map. This behavior can occur with a large number of client source entries and you add and remove the class-default class map several times in a policy map. Workaround: None.
- **CSCtr80967**—With SIP traffic running for a long period of time (for example, overnight) with a heavy volume of traffic, the ACE may encounter a few proxy map entries that leak. For example:

```
switch/Admin# sh np 1 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32767             0
Alloc Proxy Mapping:                      29612485             0
Alloc Proxy Mapping Failed:                     0             0
Release Proxy Mapping:                    29612484             0
switch/Admin# sh np 2 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32768             0
Alloc Proxy Mapping:                      33107573             0
```

```
Alloc Proxy Mapping Failed:                        0             0
Release Proxy Mapping:                      33107573             0
switch/Admin# sh np 3 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                            32766             0
Alloc Proxy Mapping:                        50967736             0
Alloc Proxy Mapping Failed:                        0             0
Release Proxy Mapping:                      50967734             0
switch/Admin# sh np 4 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                            32766             0
Alloc Proxy Mapping:                        52207388             0
Alloc Proxy Mapping Failed:                        0             0
Release Proxy Mapping:                      52207386             0

switch/Admin# sh np 1 me-stats "-D"
0 entries open.
```

Workaround: None.

- **CSCtr81263**—With high point-to-multipoint traffic, the ACE may ignore the specified connection limit specified by the **conn-limit max** command. In this case, you may observe few connections being received over the configured connection limit. Workaround: None.
- **CSCtr95088**—You may find that ND entries are not refreshed for learned entries at the configured ND interval. Workaround: None.
- **CSCtr96229**—When you remove a resource class that is associated with a specific context, in some cases the ACE may reboot. This issue is related to the number of contexts in the ACE, when the ACE configured with several contexts and a resource class, that is associated with one of the contexts, requires a sticky limit. When the ACE LB module attempts to remove the sticky entries from the free list, it first determines if there is a starving context that is waiting for resources by walking through a link list of contexts, which consumes ACE CPU time. This behavior does not occur if the resource class does not include any limits for sticky.

  Workaround: We recommend that you do not change the resource class when there is a large number of contexts or sticky groups configured in the ACE, or that you gradually change the limit in the resource class if you have configured a sticky limit.
- **CSCts09817**—In an ACE HA configuration, with an FT setup with a large configuration, when you attempt to make a configuration change, you may find that MTS buffers can leak on both the active and standby ACEs. Workaround: Do not make do any changes when you have large configurations.
- **CSCts14335**—In a redundant configuration, specification of the **np session disable** debug command puts the active ACE into the STANDBY_COLD state. Workaround: This debug command is intended only for internal debugging. Do not use the **np session disable** debug command.
- **CSCts20690**— The Internet Message Access Protocol (IMAP) probe may fail with certain IMAP servers, and the ACE displays the failure reason as "Authentication failed." In this case, the IMAP servers are configured with the name of the mailbox from which the probe retrieves e-mail through the **credentials mailbox** command. This behavior is typically encountered with SurgeMail IMAP servers, and occurs only if the IMAP server responds with multiple packets on the SELECT INBOX. Workaround: Perform one of the following actions:
  - Do not use the **credentials mailbox** command.
  - Use the IMAP TCL scripted probe.
- **CSCts24977**—The service name:snmpd(1395) terminates upon receiving signal 8. This issue can occur when polling the ACE CPU utility MIB in a loop; the snmpd process can become unresponsive and cause the ACE to reload. For this particular issue, the OID polled was .1.3.6.1.4.1.9.9.480.1.1.7.1. Workaround: Do not poll the ACE CPU utility MIB continuously in a loop.

- **CSCts25057**—Connections to a real server may not be purged with the **failaction-purge** command, and the real server enters a return code failed state. Workaround: None.
- **CSCts29208**—With one or more sticky groups and failaction reassign configured under one of the server farms, the ACE may experience the load balance issue while incrementing real server connection counts. Workaround: When this behavior occurs, do not configure the **failaction reassign** command with the server farm.
- **CSCts30483**— The ACE unexpectedly reboots. If you specify the **show version** command, the reason of the last reboot is due to the watchdog timer in the ACE:

  ```
  last boot reason:  Sibyte watchdog reload, kernel space hang
  ```

  Workaround: Use the **no system watchdog** command to disable the watchdog.
- **CSCts35928**— Back-to-back IPv6 control traffic sent to the ACE control plane for different queues does not get processed in sequence. In this case, the data queue in the ACE control plane is processed before the control queue. This behavior is seen with back-to-back IPv6 control traffic to the control plane with different Class of Service (CoS) values. Workaround: Configure the Catalyst 6500 series switch supervisor module with a CoS setting that all packets are sent to the same queue (control queue) with a higher CoS (for example, 6). In this example, a CoS of 6 causes all packets coming in on the interface (access interface only) to be processed in synchronization in the control plane.
- **CSCts36540**—In a redundant configuration, with multi-context sticky traffic, if you perform an FT switchover while under heavy traffic and the sticky database is full, the ACE will reboot. Workaround: Increase the sticky timeout value.
- **CSCts39120**—During an FT setup, you may find that VLANs are in a Down state in the ACE after you remove or add VLANs when you use the **svclc vlan-group** command. Workaround: Remove and then readd the VLANs. If necessary, repeat this process multiple times.
- **CSCts40787**—In a redundant configuration, multiple (repeated) flaps on the Catalyst supervisor engine on the FT VLAN causes the configuration controller process in the ACE to become unresponsive and the ACE reboots. Workaround: None.
- **CSCts42706**—When performing IPv6 processing, you may find that Bridge Protocol Data Units (BPDUs) are dropped by the ACE and do not get bridged. Workaround: Perform one of the following actions to resolve this issue:
  - Configure an IPv4 address.
  - Remove and then add the **ipv6 enable** command under the interface to enable IPv6 processing on the interface.
- **CSCts47978**—The ACE module may incorrectly use a custom TCL script for SSL probes with the -sslversion option. For example:

  ```
  set sock [socket -sslversion version -sslcipher cipher $ip $port]
  ```

  When this issue occurs, the following error messages can be seen in the **show script** <*script file name*> <*probe name*> command output:

  ```
  Internal error     = bad option "-sslversion": must be -async, -myaddr, -myport, or
  -server
  ```

  Workaround: Use a different keepalive type.
- **CSCts53405**—After forwarding the real server's first response packet to the client, the ACE waits for the client to send an ACK to the first response packet before forwarding subsequent server response packets. Workaround: Use the **set tcp wan-optimization rtt** command to allow you to control how the ACE applies TCP optimizations to packets on a connection associated with a Layer 7 policy map.

- **CSCts58029**—In a redundant configuration, if a context has “priority” as part of its name, this causes the Admin context to go to STANDBY COLD state. The issue is encountered only during a bulk synchronization. Workaround: Delete any context that includes “priority” in its name and rebuild it with a new name.
- **CSCts60292**—After enabling SYN-cookie-based DoS protection for an interface, when the SYN-cookie limit is reached and when a post request is sent, the request fails. In this case, the first segment reaches the server and subsequent segments get lost. Workaround: None.
- **CSCts68281**—When using a custom configured HTTPS health probe on the ACE, you may encounter the following error message:

  ```
  %ACE-3-400001: MSS mismatch from 10.0.5.193:443 (1380) to 127.1.2.34:64571 (1460) on
  interface vlan40
  ```

  Workaround: The only thing that will stop the errors is to un-apply the Remove the custom HTTPS probe from the server farm to stop the error condition.
- **CSCts69941**—With a large configuration containing a large number of contexts, interfaces, and ACLs (including a merge of individual ACLs into one large ACL), the ACE can become unresponsive 10 to 15 minutes after booting. Workaround: Specify the **show np 1 access-list resource** command after you boot the ACE. Confirm if the Leaf Parameter nodes exceeds 400K and the policy action nodes exceeds 200K (recommended values are 200K and 100K, respectively). If one of these nodes exceeds the specified value, remove the merged ACLs and associated contexts until this threshold is not exceeded in the **show np 1 access-list resource** command output.
- **CSCts79939**—The following rewrite configuration does not successfully rewrite any instances of “http” under some scenarios:

  ```
  action-list type modify http REWRITE
    header rewrite response Location header-value "(.*)http(.*)" replace "%1https%2"
  ```

  While parsing the Location header, the ACE stops parsing after encountering any instance of the first letter in the match string (“h”). At that point, the ACE does not complete the match or perform the rewrite. Workaround: None.
- **CSCts98720**—In an application where the ACE is performing firewall load-balancing with two server farms (where one server farm is for user traffic and the one is for BGP traffic sent to the firewalls), when performing a failaction reassign and then undoing the failaction, the ACE incorrectly moves a user connection to the BGP dedicated server farm. Workaround: None.
- **CSCtt02508**—An end-to-end SSL TCP connection encounters issues while uploading a large (approximately 4.5 GB) file through an ACE VIP that is configured for end-to-end SSL. Simultaneous front and back-end traces show that the ACE brings the TCP window to zero on the client side but does not send any further data toward the server on the back-end side even though the last TCP window update from the server is 65K. The upload stops and never resumes after that. Note that this issue is not seen with a Layer 4 server load-balancing VIP configuration. Workaround: None.
- **CSCtt24046**—When the ACE performs multiple simultaneous SNMP requests on the cpmProcessTable, this may result in an SNMP timeout. Workaround: Perform only sequential SNMP requests on Cisco Process MIB.
- **CSCtt33804**—During modification of an access control list (ACL) within a context, an ACL merge error may be reported on one or more of the interfaces where the ACL list is applied, leaving the interface in an inconsistent state. When this issue occurs the following system message appears:

  ```
  %ACE-1-106028: WARNING: ACL Merge failed to locate specified ACL in context 10049.
  Error while processing service-policy. Incomplete rule is currently applied on
  interface vlan200. Configuration on this interface needs to be manually reverted
  ```

Workaround: Perform one of the following actions:

  - Remove the offending lines one at a time from the ACL until the ACL can be successfully applied.
  - Reload the ACE.

- **CSCtt42497**—When performing Layer 7 server load-balancing with a configuration that includes a combination of sticky, server connection reuse, and persistence-rebalance, bad HTTP requests may occur on the server as Layer 7 HTTP packets are sent out of order. Packets sent out of order cause the server to drop the packets or tag the request as malformed. Workaround: Disable the server-conn reuse command.
- **CSCtt47587**—HTTPS probes fail only for IIS servers with client certificates mode "Accept client certificates." In this case, IIS servers with "ignore client certificates" are not impacted. Workaround: Perform one of the following actions:
  - Configure the IIS server to "ignore client certificates."
  - Configure a TCP probe instead of an HTTPS probe.
- **CSCtt76277**—In a redundant configuration, the standby ACE module is in active state when it is reloaded from the Catalyst supervisor engine through the **no power enable** or **hw module reset** command. Workaround: Perform one of the following actions:
  - Create the file "skip_reset_cde_hash_table" by specifying the following command sequence at the Catalyst:

    ```
    show clock > disk0:skip_reset_cde_hash_table
    ```

Note When the fix is out, be sure to delete the file with the **del disk0:skip_reset_cde_hash_table** command.

  - Configure an input ACL on the ACE VLAN interfaces to deny multicast traffic. For example, enter:

    ```
    access-list deny_mcast line 10 extended deny ip any 224.0.0.0 240.0.0.0
    access-list deny_mcast line 20 extended permit icmp any any
    access-list deny_mcast line 30 extended permit ip any any
    ```

- **CSCtu10624**—Establishing a Telnet connection from the ACE to a remote device is silent with no indication of a successful connection or DNS resolution. When this occurs, the lines "trying ..." and "connected..." are not seen. Workaround: None.
- **CSCtu01626**—The HTTP probe with a regex search string fails when the HTTP header is split into two packets. When this issue occurs, HTTP probes pass and fail intermittently. Workaround: The server needs to send the entire header in one receive packet and not split the header into two packets.

Software Version A5(1.1) Command Changes

Table 6 lists the command changes in software version A5(1.1).

Table 6 CLI Command Changes in Version A5(1.1)

Mode	Command and Syntax	Description
Exec	**show interface vlan** *number*	Per CSCtl53644, this command now accepts the range from 1 to 4095 to display the internal VLAN information. Previously, the range was 2 to 4094.
	show probe detail	Per CSCtj65408, the **show probe detail** command now displays the following error message in the Last disconnect err field when the server sends a regex that does not match the configured send-data value for an echo TCP or UDP probe: `Server response not matching with user configured send-data` Previously, echo probes always passed including when the server sends a regex that does not match the configured send data value.

	system watchdog hardware
	no system watchdog hardware
		Per CSCtn62319, the new **system watchdog hardware** command in Exec mode allows you to enable the SiByte hardware watchdog. By default, the hardware watchdog is disabled.
		When SiByte hardware watchdog is enabled, it restarts the ACE when the following occurs:
		• The Linux kernel becomes unresponsive and cannot receive any IOCTL messages from uspace.
		• The CP uspace becomes unresponsive and the ACE is unable to fork new processes.
		For example, to enable the hardware watchdog, enter the following command:
		`host/Admin# system watchdog hardware`
		To disable the hardware watchdog, enter the following command:
		`host/Admin# system no watchdog hardware`

Software Version A5(1.1) System Log Messages

Software version A5(1.1) includes following new system log (syslog) messages.

251010

Error Message `%ACE-3-251010: Health probe failed for server` *`address`* `on port` *`number`*`, Server response not matching with configured echo probe send-data`

Per CSCtj65408, when you configure an echo TCP or UDP probe on the ACE and the server sends a regex that does not match the configured send-data value, the probe fails and the ACE generates this syslog message.

Also the **show probe detail** command (Table 6) displays the following error message in the Last disconnect err field:

```
Server response not matching with user configured send-data
```

Previously, echo probes always passed including when the server sends a regex that does not match the configured send-data value.

Software Version A5(1.0) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(1.0):

Note Some caveats may have more than one number. A number in parentheses is a caveat number that was associated with the previous software release that now has another number for A4(2.0) and later releases.

Software Version A5(1.0) Resolved Caveats

The following resolved caveats apply to software version A5(1.0):

- **CSCtb28070 (CSCtj65690)**—When you add the **nat dynamic** *pool id* **vlan** *vlan-id* command to a Layer 3 rule (combination of Layer 3 policy map and Layer 3 class map), which already has one dynamic NAT pool configured. For example:

  ```
  policy-map multi-match pm1
  class vip1
  nat dynamic 1 vlan 731
  ```

  This configuration already contains one dynamic NAT statement. If you add another statement for NAT dynamic, that configuration will not be downloaded. Dynamic NAT configuration is not downloaded to Data Plane and dynamic NAT does not work. Workaround: Remove and add the service policy under the client interface.

- **CSCte96191 (CSCti74189)**—On a rare occasion, the route manager becomes unresponsive on the standby ACE when you attempt configuration changes similar to the following on the active ACE:
  - Remove a service policy from local to global and global to local.
  - Remove or add VIPs in a Layer 3 class map which traffic is hitting.
  - Perform a checkpoint rollback.

  Workaround: None.

- **CSCth07619** (**CSCtg30362**)—When you apply or modify ACLs or object groups to an ACE that has operated for a long time and undergone many ACL configuration changes, issues in the ACL object group expansion during the configuration download may cause an unexpected traffic drop. The **show interface** command displays a nonzero download failure counter, similar to the following:

  ```
  Access-group download failures: 8
  ```

  Workaround: Remove and re-add the object group.

- **CSCth08116**—When you configure the **expect regex** command on HTTP or HTTPS probes with a long regex string and the web page parsed by the probe is longer than 100 KB with the matched string at the bottom of the page, the probes may fail. Workaround: Configure a basic HTTP probe that does not match a regular expression.

- **CSCth15305**—During normal ACE operating conditions, the configuration manager becomes unresponsive and the ACE generates a core file. Workaround: None.

- **CSCth20813**—In a multi-threaded code, some calls are unsafe and may cause the ACE to reboot. Workaround: None.

- **CSCth23304** (**CSCth12446**)—When the ACE is using a 1-Gbps throughput license, the throughput output displayed through the **show resource** command is rounded to the nearest thousand. For example, a value of 134217728 is rounded to 134217000. This issue does not occur with other throughput licenses. Workaround: Install a throughput license that is not 1 Gbps and then uninstall the license.
- **CSCth26795**—When you configure the **mac-address autogenerate** command with the **ip dhcp relay** command on an interface, the ACE fails to relay the DHCP request to the configured server and the counters displayed by the **dhcp relay statistics** command do not increment. Workaround: Remove the **mac-address autogenerate** command from the interfaces and reboot the ACE.
- **CSCth39505** (**CSCtg85460**)—The ACE divides the sticky table and cookies between its four network processors (NPs). If a connection on one NP uses a cookie with a hash that resolves to the other NP, the NPs must perform additional inter-NP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32 KB or more of data in fewer than 10 milliseconds (msec), a zero window may result on the backend. Some server TCP stacks may inadvertently introduce a 5-second delay in this situation. The ACE should advertise a nonzero window to the sending server when the buffers are released. Workaround: You can configure the **set tcp wan-optimization rtt 0** command to apply TCP optimizations to packets for the life of a connection. However, this command results in increased resource consumption.
- **CSCth45076**—When you configure a static multicast ARP address on the ACE, you cannot ping to the address from the ACE. Workaround: None.
- **CSCth59247**—When you configure long and complex regular expressions in new or existing commands, the ACE does not allow you to make any additional changes and may become unresponsive for a long duration of time. Workaround: Shorten the regular expressions in the commands.
- **CSCth63553 (CSCtf01034)**—The standby ACE may have a higher number of connections than the active ACE. Workaround: Configure a shorter connection inactivity timeout.
- **CSCth64338**—If you configure TCP probes with small intervals and set the termination mode as forced, the TCP probe stops firing if the server sends an RST after the TCP handshake. Workaround: Remove and re-add the faulty probe from the real server.
- **CSCth64381**—When you attempt to log in to the ACE using remote authentication with a username that has special characters that are not supported by the ACE, the security process becomes unresponsive and the ACE reboots. Workaround: Do not log in to the ACE with usernames with special characters that are not supported by the ACE.
- **CSCth67961** (**CSCsy66327**)—When you enter the **show snmp group** command from any context other than the Admin context, it does not display any output. Workaround: None.
- **CSCth84690 (CSCth78715, CSCti66139)**—When you configure a large number of NAT pools and they are in use and receiving traffic, if you change the configuration to a smaller number of NAT pools, the ACE delays the release of the older NAT translation resources. For this issue to occur, the ACE must have active NAT translation objects (xlates) that are in use. The cause of this issue is the queued-up reap messages that prevent the xlate from being reaped. In this case, the configuration rollback reduced 2 K lines of NAT pools to a one-line NAT pool. The ACE generates one reap message per line for each removed NAT pool.

  Workaround: To avoid this issue, do either of the following:

  - During a configuration rollback, if the new configuration deletes a large number of NAT pools in one big pool but still keep the overall dynamic pool, remove the entire dynamic pool and re-add it when required.

  - Set up a clean checkpoint that has an empty configuration. Perform a rollback to the first configuration and then perform a rollback to the second configuration. In this case, an overall reap message cleans the resource.

  Either of the workarounds can prevent large number of reap messages from being produced and queued, which can cause the slow release of system resources.

- **CSCth89247**—When you place interfaces up and down several times or configure several interfaces or static routes, some interfaces or static routes may not work properly and connectivity to peers may be lost. Workaround: None.
- **CSCth90592**—When you configure static NAT port redirection, the ACE does not apply the configuration and displays the following error message:

  ```
  Error: A static ip and source port must be provided in ACL for static port redirection
  ```

  Workaround: Configure a source port in the ACL for static port redirection.
- **CSCti11185 (CSCth75707)**—If the client or server retransmits a packet and the remote end exceeds the acceptable window size, the ACE incorrectly drops the retransmission packet and increments the [Drops] fp TCP window left edge counter. Workaround: Disable normalization or correct the client or server to honor the window sizes.
- **CSCti11896 (CSCsv82779)**—The ACE treats the deny function inside a management policy or class map as a SKIP. The ACE does not deny the traffic. Instead, it skips the class map and tries to match another one. Workaround: None.
- **CSCti25263**—If the same SNMP request identifier is used in previous SNMP GET and GET NEXT requests to the ACE and an SNMP agent is polling the ACE, the ACE may incorrectly respond to the SNMP request. Workaround: Perform the following:
  a. Change the SNMP agent to use unique SNMP request identifiers for each SNMP request.
  b. Wait at least 10 seconds between SNMP requests that use the same SNMP request identifier.
- **CSCti40433**—When the client sends a SYN on an existing Layer 7 connection, the ACE responds to a TCP SYN with an ACK and an incorrect ACK sequence number. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing Layer 7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti61725 (CSCsz37412)**—When the software and license on the ACE are compatible, ANM does not display their compatibility status. The XML **show ft peer 1 detail** command on the ACE is not correct. Workaround: None.
- **CSCti66770** (**CSCth41583)**—When the ACE receives a cookie string that contains many cookies and encounters a space character in the cookie value, it stops processing the cookies. Spaces are not permitted in the cookie name or cookie value. Persistence or stickiness fail. Workaround: None.
- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running test case 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76422 (CSCth69782)**—When you configure a VIP on the ACE, the ARP entry is inconsistent but the connections are working. Workaround: None.
- **CSCti76678**—When you change the default destination port for an HTTP probe, the probe does not append the port to the Host tag in the HTTP request and the ACE receives an HTTP/1.1 404 Not Found error. Workaround: Configure the probe with the **header Host header-value** command to specify and append the destination port to the host in the HTTP request.

- **CSCti84218 (CSCtb03138)**—If you configure SNMP traps on a VLAN that has either the IP address or the peer IP address missing and redundancy is enabled, the active ACE does not synchronize the SNMP traps to the standby ACE. The **show ft group detail** command displays the following error:

  ```
  Error "Incremental Sync Failure: snmp config sync to sby."
  ```

  Workaround: Configure both an IP address and a peer IP address on the interface VLAN that you are using as the trap source.

- **CSCti96864 (CSCte81257)—**When you perform dynamic configurations of usernames in multiple contexts and enter the **no username** *name* command in a user context, the ACE module unexpectedly reboots and generates an SNMP core file. Workaround: None.

- **CSCtj04935**—When the Layer 7 TCP path is overutilized that causes the Timer Freelist Empty to be hit several times, the ACE reboots because of the Timer Freelist corruption. Workaround: Reduce the work load of the Layer 7 TCP path.

- **CSCtj07489**—When you configure a policy map that references another policy map on the ACE, if the checkpoint rollback or restore operation removes these recursively referenced policy maps during context deletion while the operation loads another context, the cfgmgr process may become unresponsive. This is especially risky when all context policy maps are removed which can occur during a restore operation. Workaround: None.

- **CSCtj18925 (CSCth66757)**—When you configure many servers with active/active NIC teaming, the ACE arp_mgr service may consume 100% of the CPU due to the ARP flood caused by teaming mode. Workaround: Reduce ARP traffic. Always use active/standby NIC teaming.

- **CSCtj20521 (CSCtj63624, CSCtl54241)**—If the %EARL-SWITCH_BUS_IDLE error occurs in the chassis, the supervisor declares the ACE as MajFail and the LCPFW process stops responding. The **show proc** command does not display the LCPFW process. The **reload** command on the ACE does not work. Workaround: None.

- **CSCtj30082 (CSCte91850)**—When the NPs on the ACE are in a combination of RETCODE-FAILED and INBAND-HM-FAILED state due to a traffic pattern that hashes connections to specific NPs, the **show serverfarm** *name* command displays the real servers as OPERATIONAL but they will not process any connections. Workaround: Enter the **no inservice command** and then enter the **inservice** command to restore the real server to a working state.

- **CSCtj45039**—When you configure a Session Initiation Protocol (SIP) probe for health monitoring (HM), the ACE may incorrectly display the probe as down due to the ACE using the same Call ID for multiple probe instances to different configured real servers. Workaround: Configure the ACE with a different probe type.

- **CSCtj65486 (CSCso37590, CSCtg93332)**—When you configure the mac-address autogenerate command on the client VIP interface in bridge mode, traffic to VIP starts failing. Workaround: Delete the client side interface and re-add it.

- **CSCtj68302 (CSCti13494)**—When the ACE load balances clients towards the HTTP proxies, the ACE resets proxied SSL connection; an RST on the Client Hello. This issue may be associated with HTTP/1.1 in the CONNECT request or response. Workaround: You can configure HTTP/1.0 on the client and server. Do not inspect the HTTP connections.

- **CSCtj68574**—When the ACE is processing a high rate of concurrent SSL traffic with session ID reuse, header insert, and a small session cache timeout configured, the ACE may reload. Workaround: There is no effective workaround. However, keeping the session cache timeout value at approximately 1800 to 3600 seconds can reduce the possibility of this issue occurring.

- **CSCtj80208 (CSCtl82808)**—In a redundant configuration, the active ACE30 is running A4(1.0) and the standby ACE20 is running A2(3.x). In this split mode, dynamic incremental sync is automatically disabled. After a switchover for a single user context that is configured only on the ACE30, when you try to restore a local backup of the user context that was taken on the ACE30 to the ACE20, dynamic incremental sync is enabled because the ACE20 is now active for the user context and the ACE30 reboots. Workaround: Disable dynamic incremental sync before you restore the user context configuration by entering the no ft auto-sync command. After the restore completes, enter the ft auto-sync command to trigger a bulk sync.
- **CSCtj80791**—When SIP inspection is enabled and back-to-back SIP traffic (INVITE) occurs about 4 to 5 microseconds apart with 50 to 250 calls a second or with a high rate of traffic (800 to 900 calls a second) and inspection enabled, the ACE may leak network address translations (xlates), which can cause the ACE to drop the traffic. Workaround: Avoid back-to-back UDP packets for SIP INVITE with the same five-tuple and the same call ID across a few microseconds or, if possible, disable NAT for the SIP flows.
- **CSCtj81469 (CSCtk93650)**—When there is a high rate (1000 calls per second with one request per connection) of SIP calls over TCP, a proxy-related resource leak is observed. With a lower rate of SIP TCP traffic (approximately 400 calls per second), no resource leak is observed. Workaround: Reduce the number of SIP calls per second to a lower rate.
- **CSCtj91896**—Soon after you configure a TCP probe and the probe becomes active, the server may send out-of-band data to the ACE, which causes the ACE to become unresponsive and to produce an hm_core file. Workaround: None.
- **CSCtl03706**—When the ACE performs the **snmpwalk** command on the cpmProcessTable, the **show proc cpu** command becomes unresponsive.The output of the **show system internal mts buffers** command displays an MTS leak. The output of the **show system internal mts buffers details** command confirms this leak. Also, the MTS sends error messages similar to the following:

  ```
  mts_do_msg_input() failing since no space available in 91 (src_sap = 91, opc = 1376
  PID = 934) 2
  ```

  Workaround: None.
- **CSCtl76773**—When you create a real server, class map, policy map, KAL-AP tag, server farm, or context name that includes a space in it, an ACE redundant configuration can become out of synchronization. Workaround: Do not use spaces when naming an object on the ACE.
- **CSCtl89566**—When the ACE is performing Layer 5 load balancing and receives a noncompliant HTTP request, if the request hits a default class and is Layer 4 load balanced, the ACE drops the connection. Workaround: None.
- **CSCtn11417**—On rare occasions, an XML command sent through an XML agent fails with a 500 error. This behavior can occur on an ACE software release prior to A5(1.0). Workaround: Send the XML command in raw (text) mode.

- **CSCtn40037**—The signal handler has been disabled on the network processor cores. As a result, when one core becomes unresponsive, the ACE immediately generates a core file. Typically, an ME dump would detect this and force all other cores to become unresponsive. Because the signal handler is disabled, the other cores do not get stuck and they continue to process their message queues. This behavior may be an issue when debugging customer problems. This situation happens whenever a core becomes unresponsive. Workaround: None.
- **CSCtn43569**—The CPU utilization counter that the ACE obtains from the VMware vCenter Server provides the CPU utilization of a virtual machine (VM) as a percentage of the total ESX/Hypervisor CPU utilization. This process works fine for the default case where a VM is allocated with any number of cores and no resource limits are applied. The ACE receives the correct CPU load values of the VM and the feature works as expected. However, if there are resource limits provisioned to the VM (for example, limiting it to 50 percent of the maximum CPU), the counter value that the ACE receives from the vCenter does not accurately reflect the results. For example, a VM can use the entire 50 percent of the allocated maximum CPU, and so the reported value should be 100 percent as the VM's CPU load. Instead, the reported value is 50 percent, which is the percentage of total available ESX CPU utilization.

  When you create a VM, the vCenter provides multiple options for CPU and memory allocation for the VM. As an administrator, you can allocate the number of cores to the VM and limit the CPU utilization of the VM to a portion of the maximum available CPU power (MHz). When you configure this CPU-limiting option on the vCenter, the average CPU usage counter provided by the vCenter is still calculated against the total CPU power for the ESX/ESXi host. The ACE retrieves this counter, but treats it incorrectly as the VM's CPU usage percentage against its own allocated CPU resource limit.

  Workaround: When you create a VM with a CPU resource limit that is lower than the maximum limit (MHz), adjust the CPU burst threshold that you configure on the ACE for the DWS feature to compensate for the incorrect value provided by the vCenter. Calculate the new CPU burst threshold to be configured on the ACE by using the following formula:

  > New burst threshold = expected burst threshold x VM's CPU resource limit (MHz) / VM's maximum resource limit (MHz)

- **CSCto11586**—In an ACE HA configuration, reuse connections may not be deleted on the standby ACE when the active ACE puts them on the reuse list. This behavior results in the reuse connections getting out of synchronization on the standby ACE. Workaround: None.
- **CSCto34701**—NAT translation (Xlate) entry resources may encounter a memory leak as a result of performing a checkpoint rollback. The issue may occur when your current configuration and checkpoint have NAT pools with slightly different yet overlapping IP address ranges. If you attempt to roll back the current running configuration to the previously checkpointed running configuration while there are active connections/NAT xlates, the xlates might leak. This problem could occur when a connection that is associated to an existing reaped xlate is decremented from a new xlate created against the new NAT pool. In this case, the old xlate entry reference counts stay > 0 and the xlates persist forever. Workaround: When changing the NAT pool configuration, delete the pools and wait approximately one minute before configuring a similar pool.
- **CSCto65861**—During normal ACE operating conditions, the ACE fails to reboot or to generate a file when the ha_mgr process in the ACE become unresponsive. Workaround: None.
- **CSCto83952**—The use of the packet capture function to capture packet information may sometimes generate a “Bad Merge ID” error as well as the “ACL merge add acl to list failed” error if you perform an access group deletion during the packet capture. Workaround: Delete an access group when you are not using the packet capture function.

- **CSCto98399**—ACE CLI commands may time out with configurations greater than 4000 lines. This behavior may be encountered with configurations that contain greater than 4000 lines while operating under conditions such as triggering a configuration download every 10 seconds, changing real server states, and issuing **show** commands using scripts in 10-second intervals. Workaround: Depending on the configuration size, specify a larger interval while running scripts.
- **CSCtq09823**—The ACE standby reboots when the LB_ProcessMsg receives reverse sticky traffic. In this case, the standby reboots due to a boolean being set which takes the standby ACE to the wrong code. Workaround: None.
- **CSCtq13621**—When you change a predictor under a server farm where the fail-on-all function is already configured for a real server, at least one of the real server probes is in the FAILED state and at least one of the real server probes is in the SUCCESS state, the real state moves from OPERATIONAL to PROBE_FAILED. Workaround: After changing the predictor, specify the **no fail-on-all** command followed by the **fail-on-all** command for the real server.
- **CSCtq14837**—You may find that RHI routes are not getting transferred to a new active Catalyst supervisor module. In this configuration, you have SSO setup in the Catalyst with the ACE module, and you perform an SSO switchover. Workaround: None.
- **CSCtq16302**—When small SSL record packets are sent to the ACE, the ACE dataplane may become unresponsive and the ACE reboots. Workaround: Do not send small SSL record packets to the ACE.
- **CSCtq29919**—With the **persistence-rebalance strict** command configured, when a client comes with a cookie in the first request and the comes without a cookie in the second request a memory leak to the sticky connection count can occur. Workaround: None.
- **CSCtq30198**—In an ACE HA configuration, sticky entries in the ACE standby are not removed after running overnight traffic. In this case, the active ACE does not contain any sticky entries, and the sticky database does not show any connections. Workaround: Reboot the standby ACE.
- **CSCtq32037**—An ACL download may fail as a result of you applying an access group at an interface level while removing the global access group. In this case, the ACE does not have sufficient time to synchronize the global access group deletion and, as a result, connections are dropped. Workaround: Wait for the global access group deletion to synchronize to the ACE, and then add the access group to an interface.
- **CSCtq52756—**With reverse IP sticky traffic, sticky entries may remain with an Active connection count even though no connections exist. This behavior results in a memory leak to the sticky connection count. Workaround: None.
- **CSCtq81407**—In an ACE HA configuration, in the ACE standby, certain **show** commands either fail to respond or respond after a long period of time with the error message: “System Busy:Config application in progress.” All **show** commands function properly in the active ACE. Workaround: None.
- **CSCtr03000**—In an ACE HA configuration, both the active and standby ACEs reboot when you enable sticky with the server-connection reuse feature. In this case, the ACE encounters a race condition when the ACE makes load-balancing attempts to load a conn-structure right after it has been deleted by the configuration manager, which results in the ACE rebooting. Workaround: None.
- **CSCtr22338**—When you enable SSL session ID reuse and header insert, and the client performs a GET or PUT operation on a large page, the ACE dataplane may become unresponsive and the ACE reboots. Workaround: None.
- **CSCtr26670**—When you enable SSL session ID reuse and you make an SSL-related configuration change while passing traffic, the ACE dataplane may become unresponsive and the ACE reboots. Workaround: Avoid making configuration changes when passing traffic through the ACE.

- **CSCtr32985**—With a configuration containing server connection reuse as well a sticky group, after a period of time when traffic has stopped, you may find that the ACE contains sticky entries with no connections in the connection table. In this case, the sticky entries have a timeout equal to 0 and those entries are not removed from the database. Workaround: Clear the sticky database.
- **CSCtr39117**—In an ACE HA configuration, when running HTTP traffic with the **no conn-limit** and **no rate-limit** commands configured for real servers in a server farm, in some cases when an FT switchover happens between the active and standby ACEs, you may encounter an FT flap. When this behavior occurs, you may find that all logs, context configurations, and FT configuration are deleted from the ACE. Workaround: None.
- **CSCtr44410**—After modifying the sticky resources that have been assigned to a context, even though you have allocated a specific number of sticky resources to the context, you may find that sticky entries get reused without reaching the maximum number of resources. The global pool is not used in this case, causing the removal of the existing sticky entries. Workaround: None.
- **CSCtr46599**—You may experience an HSRP flap on the ACE if your configuration includes an ACL that allows all traffic on all interfaces along with a configured default route. Workaround: Add an ACL to deny UDP traffic on port 2029.
- **CSCtr58188**—You may find that sticky entries remain in the sticky database after timeout expiration and with no active connections.Workaround: None.
- **CSCtr78693**—In some instances, SSL client connections fail to get redirected when you enable either the **authentication-failure ignore** or **authentication-failure redirect** commands to instruct the ACE the action to take when encountering a client certificate failure during the setup of the front-end connection in an SSL termination configuration. Workaround: None.
- **CSCtr94144**—Associating a class map to a policy map through XML to transmit, exchange, and interpret data among applications can sometimes result in the generation of an invalid error. Workaround: None.

Software Version A5(1.0) Open Caveats

The following open caveats apply to software version A5(1.0):

- **CSCtd42287**—When the ACE is running with the maximum limit of 8 K static entries and you remove a service policy from an interface and quickly re-add it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then re-adding it.
- **CSCte76618**—When traffic traverses the ACE module with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCtf54230**—When Layer 2-connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.
- **CSCtg87855** (**CSCtg22592**)—After you make a change to a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the **show** command.

- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.
- **CSCth46984**—When you assign VLANs to the ACE module in a Cisco Catalyst SUP-2T VSS configuration, error messages flood the supervisor console. Workaround: None.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After the ACE performs the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

  Workaround: Remove and reconfigure the real server.
- **CSCti68449** (**CSCtf43237**)—The **show xlate** command displays thousands of entries. However, the **show resource usage** command displays zero peak and zero current. Workaround: Reboot the ACE.
- **CSCti85064**—Occasionally when the ACE is under high control plane (CP) stress with a high rate of CP syslog traffic at logging Level 7, the CP becomes sluggish. If the data plane becomes unresponsive, the ACE console become unresponsive and the ACE reboots by the SME process without creating any dataplane core files. Workaround: Avoid CP syslogs at level 7 with a high rate of traffic, or enable only fast path syslogs.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

  ```
  System running low on direct mapped memory
  Please issue 'show system kcache' to diagnose further
  ```

  Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.
- **CSCtj12692**—You configure the ACE with 4000 sticky groups and do not allocate a sticky resource class. The sticky resource values are the default: minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries, you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context. After a few minutes the ACE becomes unresponsive and reboots. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj30825**—When you configure a large number of ICMP probes and directly connected hosts on the ACE, ARP resolution fails intermittently for the directly connected hosts. Workaround: Decrease the number of ICMP probes or change the ICMP probes to TCP or UDP-based probes.
- **CSCtj65408**—When you configure an ECHO TCP or UDP probe with send-data value, the probe passes even when the server sends a regex that does not match the send-data value. Workaround: You can use a TCP or UDP probe with send-data and regex values as required instead of an ECHO TCP or UDP probe.

- **CSCtj65628**—When you configure RBAC on an ACE with a custom role and domain, any permit rule allows all **show** commands to be entered regardless of the configured permissions. Workaround: None.
- **CSCtj65634**—When the maximum aclmerge instance limit of 8191 is reached and then freed, ACL merge will not occur. Also, after reaching the maximum limit of instances, if you remove the outbound ACL from the interface, the policy action nodes are not released. Workaround: None.
- **CSCtj65687**—If the VIP address conflicts with the shared interface address across contexts, the standby ACE goes into the cold state with the **show ft config-error** command displaying the following error message:

  ```
  interface vlan number
  Error: Global Policy applied, conflicts with VIP, NAT or Interface IP in shared
  interface!
  ```

  Workaround: Do not configure a VIP address with the same address as the shared interface IP address on which the service policy is configured.
- **CSCtj65693**—The **ip name-server** command is seen in the standby mode even after removing it in active mode. This issue happens in redundant configuration. Workaround: None.
- **CSCtl45638**—When you configure usernames with the ACE default roles, a user with the Network-Monitor role does not have access to some commands. Workaround: Assign the user with the admin role.
- **CSCtl54305**—When HTTP, DNS, and SIP inspection load balancing and no contexts are active on a standby ACE and the supervisor is running s72033-adventerprisek9_wan_dbg-mz.SIERRA_INTEG_101111, the supervisor logs an ACE observed storm control message, similar to the following:

  ```
  %PM_PLATFORM-5-PORTDROP: Port TenGigabitEthernet3/1 dropped packets due to storm
  control
  ```

  The message had no impact on operations. Workaround: None.
- **CSCtl68891**—When you configure a real server on the ACE, assign it an IP address, place it in service, and then delete it, the ACE generates an unnecessary trap. When the real server state changes from ARP-FAILED to operational, the ACE generates the CesRServerStateUp trap. Workaround: None.
- **CSCto34856**—When you configure Layer 7 load-balancing or HTTPS termination with sticky and redundancy on the ACE, HTTP/HTTPS Post requests with large headers that span multiple packets can cause packets to be sent to the backend servers out of order. This behavior can cause the server to drop the request to or to send a failure return-code. Workaround: Remove sticky from the server farm.
- **CSCto68956**—With the ACE configured for sticky and multiple sticky groups, and the sticky database is almost full, the ACE may unexpectedly reboot and generate a core file. When this behavior occurs, the core file points to the Load Balancing (LB) process thread where a new sticky entry is trying to be obtained. Workaround: None.
- **CSCto76442**—When you configure a new IPv6 duplicate address attempt for an interface through the **ipv6 nd dad-attempts** command, you may find that the value does not take effect. Workaround: Specify a **shut/no shut** command sequence on the interface to reenable the interface. We recommend that prior to specifying a **shut/no shut** command sequence that you keep track of the current traffic movement on the interface.
- **CSCtq67444**—You may find that the ACE is reset by the Catalyst 6500 series switch supervisor engine. In this configuration, you have SSO setup in the switch with the ACE module, and you perform an SSO switchover. Workaround: None.

- **CSCtr14599**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not being removed completely from the Catalyst 6500 series switch or Cisco 7600 series router. When this behavior occurs, debugging starts on the Catalyst series switch or router with the message "Failed to remove route." Workaround: None.
- **CSCtr24875**—When advertising an ACE module VLAN for route health injection (RHI) with an IPv6 address, you may find that RHI routes are not injected in the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior happens when your configuration includes more than 70 VIPs. You will not encounter this issue with an IPv4 address. Workaround: None.
- **CSCtr33704**—In some instances, old routes are not properly removed from the Catalyst 6500 series switch or Cisco 7600 series router supervisor engine. This behavior can occur under changes that are related to route health injection (RHI). For example:
  - When you configure a global IPv6 address on an interface and the ACE performs duplicate address detection (DAD) for the alias IP address. In this case, the ACE injects a route that corresponds to an interface IP address. Once it passes, the ACE removes the interface and injects a route that corresponds to the alias. This route is not updated properly in the supervisor engine module.
  - When you configure the ACE to advertise an ACE module VLAN for route health injection (RHI) that is different from the VIP interface VLAN, and you remove the advertised VLAN, the ACE contains the two routes.
  - In a redundant configuration, after a switchover, routes that correspond to the older ACE module are not removed.

  Workaround: Reboot the ACE module.
- **CSCtr56096**—You may observe that the sticky-conns counter in the **show serverfarm detail** command output displays a nonzero value when there are no current connections. The sticky-conns counter displays the number of active connections when using sticky and gets updated when there are one or more active (current) connections. Workaround: None.
- **CSCtr58692**—You may find that configuring the **fail-on-all** command, followed by a probe, for a real server does not function properly. Workaround: After adding or removing a probe for a real server, remove and re-add the **fail-on-all** command for the real server.
- **CSCtr70477**—You may observe that the **show service policy detail** command output includes invalid values for the Hit Count or Dropped Conns counters under the class-default class map. This behavior can occur with a large number of client source entries and when you add and remove the class-default class map several times in a policy map. Workaround: None.
- **CSCtr80967**—With SIP traffic running for a long period of time (for example, overnight) with a heavy volume of traffic, the ACE may encounter a few proxy map entries that leak. For example:

```
switch/Admin# sh np 1 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32767             0
Alloc Proxy Mapping:                       29612485            0
Alloc Proxy Mapping Failed:                      0             0
Release Proxy Mapping:                     29612484            0
switch/Admin# sh np 2 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32768             0
Alloc Proxy Mapping:                       33107573            0
Alloc Proxy Mapping Failed:                      0             0
Release Proxy Mapping:                     33107573            0
switch/Admin# sh np 3 me-stats "-s lb" | inc Mapping
Free Proxy Mapping:                          32766             0
Alloc Proxy Mapping:                       50967736            0
Alloc Proxy Mapping Failed:                      0             0
Release Proxy Mapping:                     50967734            0
switch/Admin# sh np 4 me-stats "-s lb" | inc Mapping
```

```
Free Proxy Mapping:                          32766            0
Alloc Proxy Mapping:                      52207388            0
Alloc Proxy Mapping Failed:                     0            0
Release Proxy Mapping:                    52207386            0

switch/Admin# sh np 1 me-stats "-D"
0 entries open.
```

Workaround: None.

- **CSCtr81263**—With high point-to-multipoint traffic, the ACE may ignore the specified connection limit specified by the **conn-limit max** command. In this case, you may observe a few connections being received over the configured connection limit. Workaround: None.
- **CSCtr95088**—You may find that ND entries are not refreshed for learned entries at the configured ND interval. Workaround: None.
- **CSCtr96229**—When you remove a resource class that is associated with a specific context, in some cases the ACE may reboot. This issue is related to the number of contexts in the ACE, when the ACE configured with several contexts and a resource class, which is associated with one of the contexts, requires a sticky limit. When the ACE LB module attempts to remove the sticky entries from the free list, it first determines if there is a starving context that is waiting for resources by walking through a link list of contexts, which consumes ACE CPU time. This behavior does not occur if the resource class does not include any limits for sticky.

  Workaround: We recommend that you do not change the resource class when there is a large number of contexts or sticky groups configured in the ACE, or that you gradually change the limit in the resource class if you have configured a sticky limit.
- **CSCts09817**—In an ACE HA configuration, with an FT setup with a large configuration, when you attempt to make a configuration change, you may find that MTS buffers can leak on both the active and standby ACEs. Workaround: Do not make any changes when you have large configurations.
- **CSCts25057**—Connections to a real server may not be purged with the **failaction-purge** command, and the real server enters a return code failed state. Workaround: None.
- **CSCts35928**— Back-to-back IPv6 control traffic sent to the ACE control plane for different queues does not get processed in sequence. In this case, the data queue in the ACE control plane is processed before the control queue. This behavior is seen with back-to-back IPv6 control traffic to the control plane with different Class of Service (CoS) values. Workaround: Configure the Catalyst 6500 series switch supervisor module with a CoS setting that all packets are sent to the same queue (control queue) with a higher CoS (for example, 6). In this example, a CoS of 6 causes all packets coming in on the interface (access interface only) to be processed in synchronization in the control plane.
- **CSCts39120**—During an FT setup, you may find that VLANs are in a Down state in the ACE after you remove or add VLANs when you use the **svclc vlan-group** command. Workaround: Remove and then readd the VLANs. If necessary, repeat this process multiple times.
- **CSCts42706**—When performing IPv6 processing, you may find that Bridge Protocol Data Units (BPDUs) are dropped by the ACE and do not get bridged. Workaround: Perform one of the following actions to resolve this issue:
  - Configure an IPv4 address.
  - Remove and then add the **ipv6 enable** command under the interface to enable IPv6 processing on the interface.
- **CSCts56112**—If you have dynamic workload scaling (DWS) configured in the ACE, ACE connectivity with the Cisco Nexus 7000 series switch may be lost. When this happens, SSH connection to the Cisco Nexus 7000 series switch from the ACE reports an “authentication failure” error. Workaround: Perform the following actions:

  - On the newly active Cisco Nexus 7000 series switch, assign a new management IP address.
  - On the ACE, update the IP address of the Nexus 7000 management interface for the local Nexus device on the ACE to the newly assigned IP address.

- **CSCts76353**—In some cases, you may find that real servers frequently reach the INBAND-FAIL state. This issue occurs because the reset interval in the inband health monitoring function is working in seconds instead of milliseconds, which causes the error interval detection to be longer and increases the chance of hitting the INBAND-FAIL state. There are no issues with the other associated real server timers (such as reset, resume-service, and so on) are all working properly. Workaround: None.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.