Techical Note

Migrating the Cisco Application Control Engine

Customers are eager to adopt the new Cisco® Application Control Engine ACE30 module, which offers significantly higher performance, IPv6 support, and tighter integration with Cisco Nexus® 7000 Series Switches when compared to the previous Cisco ACE10 and ACE20 modules. This document is intended to help facilitate the adoption of the Cisco ACE30 module in existing Cisco ACE module environments. It provides a guided walk-through for seamless Cisco ACE migration, a worksheet for implementing a Cisco ACE migration, an overview of what is new in the Cisco ACE30 module, and an explanation of important differences between the Cisco ACE30 modules and previous modules.

Contents

Benefits of an ACE Migration **3**

ACE Migration Overview **3**

Confirming Prerequisites **3**

Staging Cisco ACE30 Modules **6**

Backups and Code Download 6
Stage the ACE30a (Will Be the Primary) 7
Stage ACE30b (Will Be the Backup) 11

Migrate the Production Environment **15**

Migrate Backup ACE10 or ACE20 to ACE30 15
Migrate Primary ACE10 or ACE20 to ACE30 17

What's New in the Cisco ACE30 Module? **20**

Detailed CLI Changes Between the Cisco ACE Software Release A2.3.x and A5.1.x **22**

New ACE Commands (Not Including IPv6) 23
New ACE show Commands 26

Cisco ACE Migration Worksheet **34**

Prerequisite Confirmation 34
Staging the Cisco ACE30 Modules 35
Migrating to the Cisco ACE30 Modules 38

Benefits of an ACE Migration

The Cisco ACE30 module for the Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers is an industry-leading application switch, increasing the availability, accelerating the performance, and enhancing the security of data center applications. The Cisco ACE30 module allows enterprises and service providers to benefit from higher performance and a richer feature set compared to the Cisco ACE10 and Cisco ACE20 modules. The benefits of the Cisco ACE30 module include:

- Double server-load-balancing (SLB) connections-per-second (CPS) performance
- Double Secure Sockets Layer (SSL) transactions-per-second (TPS) performance and throughput
- Addition of up to 6 Gbps of HTTP compression
- New licensing structure that unlocks all ACE30 module capacity by bandwidth
- IPv6 dual-stack and translation
- Nexus 7000 Integration with Dynamic Workload scaling

ACE Migration Overview

The Cisco ACE migration process is an extension of the well known software upgrade process. The process has three parts: confirming prerequisites, staging the Cisco ACE30 modules, and migrating the Cisco ACE10 or ACE20 configuration to Cisco ACE30 modules. While Cisco ACE migration requires onsite support, because of the need to physically replace the ACE10 or ACE20 modules with the Cisco ACE30 modules, it follows the standard process used in hitless software upgrades. The following highlights of the Cisco ACE migration process will be covered in detail:

- Backing up existing Cisco ACE10/20 modules
- Staging Cisco ACE30 modules
- Migrating the backup Cisco ACE10 or ACE20 modules to Cisco ACE30 modules
- Making the backup Cisco ACE30 module active
- Migrating the primary Cisco ACE10 or ACE20 module to Cisco ACE30 module
- Making the primary Cisco ACE30 Module active

The Cisco ACE migration process provides a seamless migration from the Cisco ACE10 and ACE20 to the new Cisco ACE30 modules helping to ensure a hitless Layer 4 migration to Cisco ACE30. While proxied connections will be affected during the two forced failovers during the migration, you can maintain client persistence if you configure it. This helps to ensure client session resumption of proixed connections after each failover event.

Confirming Prerequisites

The first step in the Cisco ACE migration process is to define the migration prerequisites. This lays the ground-work for a successful and uneventful migration experience. The prerequisites for a Cisco ACE migration consist of: verifying Cisco IOS® Software versions, making backups of Cisco ACE, verifying access to backup servers, locating the proper staging area, and understanding the impact to client/server traffic during the migration process. It is very important to use the **Cisco ACE Migration Worksheet**, found at the end of this document, to help ensure a successful Cisco ACE migration.

A maintenance window is highly recommended for the Cisco ACE migration process. While the migration has minimal impact on production traffic, a maintenance window should be used for this process, as it would be for code upgrade processes.

In planning for the amount of time required for the migration, you can base this on previous software upgrade experiences. In internal testing, we have found that a one-hour period provides sufficient time to migrate the Cisco ACE10 and ACE20 modules to Cisco ACE30 modules. This one-hour timeframe accounts for the Cisco ACE30 module load times and typically leaves 30 minutes to validate that the migration is working as expected. The rule of thumb is to add approximately 30 minutes to your typical software upgrade maintenance window to account for the physical swapping of the Cisco ACE modules and subsequent boot time.

Determine the staging environment that will be used for the Cisco ACE30 modules. In order to minimize downtime and risk, it is highly recommend that the Cisco ACE30 modules be staged prior to the actual migration process. Although staging is not required, it helps ensure a successful and less stressful Cisco ACE migration.

The first step is to determine where the Cisco ACE30 modules can be staged. We recommend that you use a lab or other nonproduction environment where you are running a Cisco Catalyst 6500 Series with a free slot and a Supervisor Engine 720. This area will need to have access to the backup files that will be created in the staging process. The area should be completely isolated from production traffic and production VLANs. You can achieve this isolation by simply not sharing the production VLANs with the Cisco ACE30 modules being staged. Staging isolation will help ensure there are no duplicate IPs or networking loops that can impact production traffic.

Verify the existing production environment Cisco IOS® Software versioning. In both the staging area and production environment, the Cisco Supervisor Engine 720 must be running the minimum level of Cisco IOS code to support the new Cisco ACE30 module. The ACE30 requires a minimum Cisco IOS Software train in order for the Supervisor to recognize the ACE30 module. The following list summarizes the comprehensive Chassis, Supervisor Engine, and IOS Support table found in the **Release Note vA4(2.x), Cisco ACE Application Control Engine Module**:

- Catalyst 6500 Sup720 Cisco IOS Software Release 12.2(33)SXI4 (or later)
- Catalyst 7600 Sup720 Cisco IOS Software Release 15.0(1)S (or later)
- Catalyst 7600 RSP720 Cisco IOS Software Release 15.0(1)S (or later)

Since the Cisco ACE30 module uses a new label identifying the new hardware, the image for the Cisco Catalyst Supervisor Engine's IOS Software must be upgraded to support the new label before it can recognize the Cisco ACE30 module.

While there are no mandatory requirements on Cisco ACE 10 or ACE20 code for the migration process, it is hihgly recommended A2.3.1 or later Cisco ACE Software image be used to enable backup and restore capabilities on the Cisco ACE10 or ACE20 module. The migration process described below is based upon the A2.3.1 or later Cisco ACE Software image.

Provide access to the Cisco ACE backup server and backup server for nonexportable SSL key files, if used. The Cisco ACE30 modules will need access to the backup file made from the production Cisco ACE10 or ACE20 modules, in order to restore the configurations during the staging process. Thus access to the Cisco ACE backup server is a mandatory requirement.

For customers using Cisco ACE for SSL offloading, be aware that only exportable SSL files can be automatically backed up using the Cisco ACE. This means if SSL keys were created on or imported to the Cisco ACE with the nonexportable option, they will need to be manually restored or recreated during the staging process, as they will not be exportable from ACE directly. To verify the SSL file state, use the **show crypto files** command in each Cisco ACE context. In the following example, notice that the Admin context has a SSL key (secure-server.key) that was imported with the nonexportable parameter:

```
ACE10/20-pri/Admin# show crypto files
Filename                                  File   File     Expor      Key/
                                          Size   Type     table      Cert
------------------------------------------------------------------------
cisco-sample-cert                         1082   PEM      Yes        CERT
cisco-sample-key                          887    PEM      Yes         KEY
secure-server.crt                         2464   PEM      Yes        CERT
secure-server.key                         1679   PEM      No          KEY
```

Verify the fault-tolerant (FT) deployment model (active/standby or active/active) and use of preemption in the FT groups. In the migration phase of the Cisco ACE migration process, the virtual contexts will need to be active on a single Cisco ACE as Cisco ACE modules are physically swaped. You must therefore disable preemption to enable a manual fault-tolerant failover of contexts. It also prevents an unexpected or premature failover during the Cisco ACE migration process, which can have an unexpected impact on client-server traffic.

Before proceeding to the next step in the Cisco ACE migration process, it important to **understand the impact migration may have on active client-server traffic**. The Cisco ACE module is designed to take full advantage of network processors to process flows quickly and efficiently for simple Layer 3 and Layer 4 load balancing, as well as application- aware (Layer 7) load balancing. Client flows, or connections, require varying levels of processing and memory depending upon how they are handled within the Cisco ACE module. Table 1 shows the levels of flow processing along with the type of processing per level, and the features or functionality provided at each level of processing.

Table 1. Flow Processing Levels

Level of Flow Processing	Type of Processing	Feature or Function
Layer 3 and Layer 4	Balancing on first packet Applies to TCP/UDP for L4 rules Applies to all other IP protocols	Basic load balancing (LB) Source IP sticky TCP/IP normalization Select server or farm based on source IP
Layer 7 TCP Splicing (Un-proxy)	Terminate TCP connection Buffer request, inspect, LB Create hardware shortcut	HTTP L7 rules on first request (URL LB) Cookie sticky (persistence) Generic TCP payload parsing
Layer 7 Re-proxy	TCP splicing + ability to parse subsequent HTTP requests within same TCP	HTTP L7 rules with HTTP 1.1 connection keepalive (“persistence rebalance”)
Layer 7 Full Proxy	Fully terminate client TCP connections	SSL offload TCP re-use HTTP 1.1 pipelining Protocol inspections (FTP, SIP, DNS, …)

During the Cisco ACE migration process, there will be two forced failover events. For all Layer 3 and Layer 4 traffic, there will be no significant impact to active connections as connection flow information and sticky persistence tables are replicated to the backup ACE. For connections requiring Layer 7 TCP Splicing and Re-proxy, there is a chance they will be impacted by the failover events. These flows have essentially two phases: one is a Layer 7 inspection phase and the second is the Layer 4 data transmission phase. If the connection is being inspected at Layer 7 at the time of the failover event, the connection will be impacted by the event. If the connection is a Full Proxy connection, it will also be impacted during the failover event. For all Layer 7 processed flows, persistence can be maintained provided sticky replication has been configured.

This concludes the prerequisite checklist. Be sure to verify that the system meets the minimum requirements for the Cisco IOS Software Release before proceeding to the next step in the migration process.

Staging Cisco ACE30 Modules

The second step in the migration process is to stage the new Cisco ACE30 modules. This pre-migration step allows the ACE30 modules to be staged offline in a lab without the pressures of a maintenance window or downtime. The staging process steps are as follows.

Backups and Code Download

Step 1. Using the Cisco CLI or Application Networking Manager (ANM), backup the active and standby Cisco ACE10 or ACE20 modules:

```
ACE-pri/Admin# backup all

Backup started. Use show commands for status information.

ACE-pri/Admin# show backup status


Backup Archive: 20a-ace-sol_2011_09_12_23_29_09.tgz

Type          : Full

Start-time    : Mon Sep 12 23:29:58 2011

Finished-time : Mon Sep 12 23:29:09 2011

Status        : SUCCESS

Current vc    : web-apps

Completed     : 11/11
```

Step 2. Export the backup files to a FTP/SFTP server. The Cisco ACE30 modules in staging must be able to reach the FTP or SFTP server to restore the configurations:

```
ACE-pri/Admin# copy backup-all sftp://172.25.91.127

Enter the destination filename[]? [ACE-pri_2011_09_12_23_29_09.tgz] 20a-
primary.tgz

Enter username[]? root

Connecting to 172.25.91.127...

Warning: Permanently added '172.25.91.127' (RSA) to the list of known hosts.
```

```
root@172.25.91.127's password:
sftp> Uploading /TN-HOME/Admin/ACE-pri_2011_09_12_23_29_09.tgz to /root/20a-primary.tgz
/TN-HOME/Admin/ACE-pri_2011_09_12_23_29 100%   24KB   0.0KB/s   00:00

ACE-sec/Admin# copy backup-all sftp://172.25.91.127
Enter the destination filename[]? [ACE-sec_2011_09_12_26_49_09.tgz] 20b-secondary.tgz
Enter username[]? root
Connecting to 172.25.91.127...
Warning: Permanently added '172.25.91.127' (RSA) to the list of known hosts.
root@172.25.91.127's password:
sftp> Uploading /TN-HOME/Admin/ACE-sec_2011_09_12_26_49_09.tgz to /root/20b-secondary.tgz
/TN-HOME/Admin/ACE-sec_2011_09_12_26_49 100%   24KB   0.0KB/s   00:00
```

Step 3. Download the A4.2.1a version of the Cisco ACE image from Cisco.com

http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Application+Control+Software&mdfid=280557289&treeName=Cisco+Interfaces+and+Modules&mdfLevel=SERIES&url=null&modelName=Cisco+ACE+Application+Control+Engine+Module&isPlatform=N&treeMdfId=268437717&modifmdfid=null&imname=&hybrid=Y&imst=N

Stage the ACE30a (Will Be the Primary)

Step 1. Physically install a new Cisco ACE30 module into Cisco Catalyst 6500 Series chassis within the staging area. This Cisco ACE30 module will be referenced as "ACE30a" hence forth.

Step 2. Log into the ACE from the Supervisor Engine 720 and configure an interface and IP address to allow the ACE to connect to the backup server where the ACE10 or ACE20 backup files were stored in the preceding staging steps. If needed, add the appropriate default route to access backup servers if they are a hop away. Note: Neither ACLs nor management policies need to be configured because the Cisco ACE will initialize the outgoing connections in the staging process.

Step 3. Install the A4.2.1a Cisco ACE Software image on ACE30a:

```
switch/Admin# copy sftp://172.25.91.127 image:
Enter source filename[]? c6ace-t1k9-mz.A4_2_1a.bin
Enter the destination filename[]? [c6ace-t1k9-mz.A4_2_1a.bin]
Enter username[]? root
Connecting to 172.25.91.127...
The authenticity of host '172.25.91.127 (172.25.91.127)' can't be established.
RSA key fingerprint is 77:fd:f3:1a:7e:9f:06:7e:79:82:62:45:09:f7:db:35.
```

```
Are you sure you want to continue connecting (yes/no)? yes
root@172.25.91.127's password:
sftp> Fetching /images/ c6ace-t1k9-mz.A4_2_1a.bin to /mnt/cf/ c6ace-t1k9-
mz.A4_2_1a.bin
/images/c6ace-t1k9-mz.A4_2_1a.bin              100%   56MB   2.1MB/s   00:26
```

Step 4. Restore the backup of the primary ACE10/20 to ACE30a . Disregard the warning about the licensing file, which is a normal part of the migration process. Note that the ACE30a command prompt will change immediately after the restore begins. This is due to the Cisco ACE hostname being restored. Again this is an expected behavior.

```
switch/Admin# copy sftp://172.25.91.127 disk0:
Enter source filename[]?20a-primary.tgz
Enter the destination filename[]? [20a-primary.tgz]
Enter username[]? root
Connecting to 172.25.91.127...
The authenticity of host '172.25.91.127 (172.25.91.127)' can't be established.
RSA key fingerprint is 77:fd:f3:1a:7e:9f:06:7e:79:82:62:45:09:f7:db:35.
Are you sure you want to continue connecting (yes/no)? yes
root@172.25.91.127's password:
sftp> Fetching /configs/20a-primary.tgz n to /mnt/cf/20a-primary.tgz
/configs/20a-primary.tgz                       100%   24KB   2.1MB/s   00:26


switch/Admin# restore all disk0:20a-primary.tgz
Warning: Archive contains incompatible licenses, ignoring license restore.
Restore started. Use show commands for status information.
ACE-pri/Admin#

NOTE: Processing has started for applied config


NOTE: Processing has finished for applied config

ACE-pri/Admin#
ACE-pri/Admin# show restore status
```

```
Backup Archive: ACE10/20a-primary.tgz
Type          : Full
Start-time    : Mon Sep 12 23:31:44 2011
Finished-time : Mon Sep 12 23:31:59 2011
Status        : SUCCESS
Current vc    : web-apps
Completed     : 11/11
ACE-pri/Admin#
```

Step 5. Install the bandwidth license for the Cisco ACE30 module if applicable:

```
ACE30/Admin# copy sftp://172.25.91.127 disk0:
Enter source filename[]? ACE30-MOD-16-K9.lic
Enter the destination filename[]? [ACE30-MOD-16-K9.lic]
Enter username[]? root
Connecting to 172.25.91.127...
root@172.25.91.127's password:
sftp> get ACE30-MOD-16-K9.lic /TN-HOME/Admin/ACE30-MOD-16-K9.lic
/licenses/ACE30-MOD-16-K9.lic                  100%   56MB   2.1MB/s   00:26
sftp> exit

ACE30/Admin# dir disk0:

  191 Sep 10 2011 10:24:26 ACE30-MOD-16-K9.lic
 1024 May 09 2010 16:21:47 cv/
    0 Jan 01 2000 00:03:50 kernel_log_messages1.txt
89401 Jan 01 2000 00:03:48 sysmgr_info

           Usage for disk0: filesystem
                    1164288 bytes total used
                   10000384 bytes free
                   11164672 bytes total

ACE30/Admin# license install disk0:ACE30-MOD-16-K9.lic
```

Step 6. Modify boot string to load the A4.2.1a Cisco ACE Software image. Since the Cisco ACE10 or ACE20 configuration was restored, the boot string is referencing the Cisco ACE10 or ACE20 image, which will not load on the Cisco ACE30. View the current boot string, and then add the new boot string referencing the A4.2.1a image. Then remove the previous boot string for the Cisco ACE10 or ACE20 image:

```
ACE-pri/Admin# show run | inc boot
Generating configuration....
boot system image:c6ace-t1k9-mz.A2_3_4.bin
ACE-pri/Admin(config)# boot system image:c6ace-t1k9-mz.A4_2_1a.bin
ACE-pri/Admin(config)# no boot system image:c6ace-t1k9-mz.A2_3_4.bin
ACE-pri/Admin(config)# exit
```

Step 7. Create a checkpoint of the ACE configuration, so it can be restored after the production environment is migrated to the Cisco ACE30 modules.

```
ACE-pri/Admin# checkpoint create cfg-preempt
Generating configuration....
Created configuration checkpoint 'cfg-preempt'
```

Step 8. If the Admin context has **preempt** configured within the FT groups, then it must be removed to allow manual context failover and to prevent a premature failover during the Cisco ACE migration process. The best way to ensure the **no preempt** command is applied to all FT groups is to copy the **show run ft | inc group** output to an editor and append a newline with the **no preempt** command. Then paste the result back into the Admin context:

```
ACE-pri/Admin# show run ft | inc group
Generating configuration....
ft group 1
ft group 2
ft group 3
ft group 4
```

In a text editor add a newline after each FT group and the command **no preempt:**

```
ft group 1
no preempt
ft group 2
no preempt
ft group 3
no preempt
ft group 4
no preempt
```

Copy and paste the result into the ACE-pri (ACE30a) Admin context:

```
ACE-pri/Admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ACE-pri/Admin(config)# ft group 1
ACE-pri/Admin(config-ft-group)# no preempt
ACE-pri/Admin(config-ft-group)# ft group 2
ACE-pri/Admin(config-ft-group)# no preempt
ACE-pri/Admin(config-ft-group)# ft group 3
ACE-pri/Admin(config-ft-group)# no preempt
ACE-pri/Admin(config-ft-group)# ft group 4
ACE-pri/Admin(config-ft-group)# no preempt
```

Step 9. Save the ACE configuration and reload the Cisco ACE30 module to ensure that it boots the new image as expected:

```
ACE-pri/Admin# wr mem all
Generating configuration....
running config of context Admin saved
Generating configuration....

ACE-pri/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
Generating configuration....
running config of context Admin saved
Generating configuration....
Perform system reload. [yes/no]: [yes]
```

Stage ACE30b (Will Be the Backup)

Step 1. Physically install a new Cisco ACE30 modules into the Cisco Catalyst 6500 Series chassis. This Cisco ACE30 module will be referenced as “ACE30b” hence forth.

Step 2. Log into the ACE from the Supervisor Engine 720 and configure an interface and IP address to allow the ACE to connect to the backup server where the ACE10 or ACE20 backup files were stored in the prededing staging steps. Add the appropriate default route to access backup servers if they are a hop away. Note: Neither ACLs nor management policies need to be configured as the ACE will initiate the outgoing connections in the staging process.

Step 3. Install the A4.2.1a Cisco ACE Software image on ACE30b:

```
switch/Admin# copy sftp://172.25.91.127 image:
Enter source filename[]? c6ace-t1k9-mz.A4_2_1a.bin
Enter the destination filename[]? [c6ace-t1k9-mz.A4_2_1a.bin]
Enter username[]? root
Connecting to 172.25.91.127...
The authenticity of host '172.25.91.127 (172.25.91.127)' can't be established.
RSA key fingerprint is 77:fd:f3:1a:7e:9f:06:7e:79:82:62:45:09:f7:db:35.
Are you sure you want to continue connecting (yes/no)? yes
root@172.25.91.127's password:
sftp> Fetching /images/ c6ace-t1k9-mz.A4_2_1a.bin to /mnt/cf/ c6ace-t1k9-
mz.A4_2_1a.bin
/images/c6ace-t1k9-mz.A4_2_1a.bin             100%   56MB   2.1MB/s   00:26
```

Step 4. Restore the backup of the primary ACE10 or ACE20 to ACE30b. Disregard the warning about the licensing file, which is a normal part of the Cisco ACE migration process. Note that the ACE30b command prompt will change immediately after the restore begins. This is due to the Cisco ACE hostname being restored. Again this is an expected behavior:

```
switch/Admin# copy sftp://172.25.91.127 disk0:
Enter source filename[]?20b-secondary.tgz
Enter the destination filename[]? [20b-secondary.tgz]
Enter username[]? root
Connecting to 172.25.91.127...
The authenticity of host '172.25.91.127 (172.25.91.127)' can't be established.
RSA key fingerprint is 77:fd:f3:1a:7e:9f:06:7e:79:82:62:45:09:f7:db:35.
Are you sure you want to continue connecting (yes/no)? yes
root@172.25.91.127's password:
sftp> Fetching /configs/20b-secondary.tgz to /20b-secondary.tgz
/configs/20b-secondary.tgz                    100%   24KB   2.1MB/s   00:26


switch/Admin# restore all disk0:20b-secondary.tgz
Warning: Archive contains incompatible licenses, ignoring license restore.
Restore started. Use show commands for status information.
ACE-sec/Admin#
```

```
NOTE: Processing has started for applied config


NOTE: Processing has finished for applied config

ACE-sec/Admin#
ACE-sec/Admin# show restore status

Backup Archive: ACE10/20b-secondary.tgz
Type          : Full
Start-time    : Mon Sep 12 23:51:59 2011
Finished-time : Mon Sep 12 23:52:17 2011
Status        : SUCCESS
Current vc    : web-apps
Completed     : 11/11
ACE-sec/Admin#
```

Step 5. Install the bandwidth license for the Cisco ACE30 module if applicable:

```
ACE30/Admin# copy sftp://172.25.91.127 disk0:
Enter source filename[]? ACE30-MOD-16-K9.lic
Enter the destination filename[]? [ACE30-MOD-16-K9.lic]
Enter username[]? root
Connecting to 172.25.91.127...
root@172.25.91.127's password:
sftp> get ACE30-MOD-16-K9.lic /TN-HOME/Admin/ACE30-MOD-16-K9.lic
/licenses/ACE30-MOD-16-K9.lic                  100%   56MB   2.1MB/s   00:26
sftp> exit

ACE30/Admin# dir disk0:

  191 Sep 10 2011 10:24:26 ACE30-MOD-16-K9.lic
 1024 May 09 2010 16:21:47 cv/
    0 Jan 01 2000 00:03:50 kernel_log_messages1.txt
89401 Jan 01 2000 00:03:48 sysmgr_info
```

```
                Usage for disk0: filesystem
                         1164288 bytes total used
                        10000384 bytes free
                        11164672 bytes total

ACE30/Admin# license install disk0:ACE30-MOD-16-K9.lic
```

Step 6. Modify the boot string to load the A4.2.1a software image. Since the Cisco ACE10 or ACE20 configuration was restored, the boot string is referencing the Cisco ACE10 or ACE20 image, which will not load on the Cisco ACE30. View the current boot string, and then add the new boot string referencing the A4.2.1a image. Then remove the previous boot string for the Cisco ACE10/20 image:

```
ACE-sec/Admin# show run | inc boot
Generating configuration....
boot system image:c6ace-t1k9-mz.A2_3_4.bin
ACE-sec/Admin(config)# boot system image:c6ace-t1k9-mz.A4_2_1a.bin
ACE-sec/Admin(config)# no boot system image:c6ace-t1k9-mz.A2_3_4.bin
ACE-sec/Admin(config)# exit
```

Step 7. If the Admin context has preempt configured within the FT groups, it must be removed to allow manual context failover and to prevent a premature failover during the Cisco ACE migration process. The best way to ensure the **no preempt** command is applied to all FT groups is to copy the **show run ft | inc group** output to a editor and append a newline with the **no preempt** command, then paste it back into the Admin context. See Step 6 in the “Stage ACE30a” section for details.

Step 8. Save the ACE configuration and reload the Cisco ACE30 module to ensure that it boots the new image as expected.

```
ACE-sec/Admin# wr mem all
Generating configuration....
running config of context Admin saved
Generating configuration....

ACE-sec/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
Generating configuration....
running config of context Admin saved
Generating configuration....
Perform system reload. [yes/no]: [yes]
```

Migrate the Production Environment

The last step in the migration process is to replace the Cisco ACE10 or ACE20 modules with the staged Cisco ACE30 modules. This is a simple process providing a hitless migration for the majority of client connections. Follow these steps.

Migrate Backup ACE10 or ACE20 to ACE30

Step 1. On the primary (active) Cisco ACE10 or ACE20 module, create a checkpoint for the current configuration.

```
ACE-pri/Admin# checkpoint create pri-orig
Generating configuration....
Created configuration checkpoint 'pri-orig'
```

Step 2. If the Admin context on the primary Cisco ACE10 or ACE20 module has preempt configured within its FT groups, then they must be removed to allow manual context failover and to prevent a premature failover during the Cisco ACE migration process. The best way to ensure "no preempt" is applied to all ft groups is to copy the **"show run ft | inc group"** output to a editor and append a newline with "no preempt", then paste it back into the Admin context. See step 6 in the Stage ACE30a section above for more details.

Step 3. Power-down the backup ACE10 or ACE20 from the secondary Cisco Catalsyt Supervisor Engine 720.

```
cat6k-sec#show module services
  Module          Model                   Services
----------   -----------------     --------------------
    1        ACE10/20-MOD-K9           ACE-16G-LIC ACE-VIRT-250 ACE-SSL-15K-K9

cat6k-sec#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cat6k-sec(config)#no power enable module 1
%Power admin state updated
```

Step 4. Physically replace the backup Cisco ACE10 or ACE20 module with the Cisco ACE30b module.

Step 5. Power-on ACE30b. The ACE30b will boot as standby.

```
cat6k-sec(config)#power enable module 1
%Power admin state updated
cat6k-sec(config)#exit
```

Step 6. Once ACE30b is warm perform the ACE10 or ACE20 failover.

```
cat6k-sec#session s 1 p 0
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
```

```
Trying 127.0.0.10 ... Open

ACE-sec login: admin
Password:


NOTE: Configuration mode has been disabled on all sessions

Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
ACE-sec /Admin# show ft group brief

FT Group ID: 1  My State:FSM_FT_STATE_STANDBY_WARM      Peer
State:FSM_FT_STATE_ACTIVE
               Context Name: Admin     Context Id: 0   Running Cfg Sync
Status: Successful

FT Group ID: 2  My State:FSM_FT_STATE_STANDBY_WARM      Peer
State:FSM_FT_STATE_ACTIVE
               Context Name: web-apps   Context Id: 3   Running Cfg Sync
Status: Successful

ACE-sec/Admin# ft switchover all
This command will cause card to switchover (yes/no)?  [no] yes

NOTE: Configuration mode is enabled on all sessions

NOTE: Configuration mode has been disabled on all sessions

NOTE: Configuration mode is enabled on all sessions
```

Step 7. Verify the FT group transition using the **show ft group brief** command. All the FT groups should show a "My State" as active and the "Sync Status" as "Successful":

```
ACE-sec/Admin# show ft group brief
FT Group ID: 1  My State:FSM_FT_STATE_ACTIVE    Peer
State:FSM_FT_STATE_STANDBY_WARM
                Context Name: Admin     Context Id: 0   Running Cfg Sync
Status: Successful

FT Group ID: 2  My State:FSM_FT_STATE_ACTIVE    Peer
State:FSM_FT_STATE_STANDBY_WARM
                Context Name: web-apps   Context Id: 3   Running Cfg Sync
Status: Successful
ACE-sec/Admin#
```

Migrate Primary ACE10 or ACE20 to ACE30

Step 1. Power down the primary ACE10 or ACE20 from the primary Cisco Catalyst Supervisor Engine720:

```
cat6k-pri#show module services
  Module          Model                  Services
----------   -----------------     --------------------
    1        ACE10/20-MOD-K9           ACE-16G-LIC ACE-VIRT-250 ACE-SSL-15K-K9

cat6k-pri#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cat6k-pri(config)#no power enable module 1
%Power admin state updated
```

Step 2. Physically replace the primary Cisco ACE10 or ACE20 module with the Cisco ACE30a module:

Step 3. Power on ACE30a. The ACE30a will boot as standby.

```
cat6k-pri(config)#power enable module 1
%Power admin state updated
cat6k-pri(config)#exit
```

Step 4. Once ACE30a is in the “STANDBY_HOT” state, perform the ACE30b failover

```
cat6k-pri#session s 1 p 0
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.10 ... Open

ACE-pri login: admin
Password:



NOTE: Configuration mode has been disabled on all sessions

Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
ACE-pri /Admin# show ft group brief

FT Group ID: 1  My State:FSM_FT_STATE_STANDBY_HOT       Peer
State:FSM_FT_STATE_ACTIVE
                Context Name: Admin     Context Id: 0   Running Cfg Sync
Status: Successful

FT Group ID: 2  My State:FSM_FT_STATE_STANDBY_HOT       Peer
State:FSM_FT_STATE_ACTIVE
                Context Name: web-apps   Context Id: 3   Running Cfg Sync
Status: Successful
```

Note: A “My State” of warm or cold, is often an indicator of a licensing or configuration error.

```
ACE-pri/Admin# ft switchover all
This command will cause card to switchover (yes/no)?  [no] yes

NOTE: Configuration mode is enabled on all sessions

NOTE: Configuration mode has been disabled on all sessions

NOTE: Configuration mode is enabled on all sessions
```

Step 5. Verify the FT group transition using the **show ft group brief** command. All FT groups should show a “My State” as active and the Sync Status” as “Successful”:

```
ACE-pri/Admin# show ft group brief
FT Group ID: 1  My State:FSM_FT_STATE_ACTIVE     Peer
State:FSM_FT_STATE_STANDBY_HOT
                Context Name: Admin     Context Id: 0   Running Cfg Sync
Status: Successful

FT Group ID: 2  My State:FSM_FT_STATE_ACTIVE     Peer
State:FSM_FT_STATE_STANDBY_NOT
                Context Name: web-apps   Context Id: 3   Running Cfg Sync
Status: Successful
```

Step 6. Roll back the checkpoint created in the section “Stage ACE30a” to roll back the previous preemption settings in each FT group:

```
ACE-pri/Admin# checkpoint rollback cfg-preempt
----------------------------------------------------------------------
-- This operation will rollback the system's running-config to the --
-- checkpoint's configuration. This can take sometime depending on --
-- the amount of diff between the two configurations.              --
----------------------------------------------------------------------
Do you wish to proceed? (y/n)  [n] y
Config rollback in progress...done.
ACE-pri/Admin#
```

```
NOTE: Processing has started for applied config

NOTE: Processing has finished for applied config
```

Step 7. Save the restored configuration, and the configurations for all other contexts.

```
ACE-pri/Admin# wr mem all
```

What's New in the Cisco ACE30 Module?

Cisco ACE30 module adds to existing features in the Cisco ACE10 ACE20 module Software Release train 2(3.x) and Cisco ACE 4710 Software Release train 3(2.x), bringing parity to the features available on the two separate hardware form factors.

The Cisco ACE30 module significantly increases the connection per second (CPS) performance typically doubling the CPS performance of the Cisco ACE10 orACE20 modules. Secure Socket Layer (SSL) offloading performance is also double the SSL transactions-per-second (TPS) rate and SSL bulk throughput of the previous generation of Cisco ACE modules. Customers adopting end-to-end SSL solution can scale much further as the Cisco ACE30 module provide an order of magnitude increase in SSL TPS performance in common end-to-end SSL deployment scenarios.

In addition to offering a significant boost to Cisco ACE performance, the Cisco ACE30 module provides a wide range of new functionality. The following is a high-level summary of the new features available on the Cisco ACE30 module:

- **HTTP compression:** Support for the following output file formats: GZIP (RFC1952), X-GZIP (RFC2616) and ZLIB (aka DEFLATE) RFC1950 for HTTP 1.1.
- **IPv6:** Dual-stack and Network Address Translation (NAT) capabilities on the Cisco ACE product family allow customers to seamlessly migrate their networks as the demand for IPv6 traffic increases.
- **Dynamic workload scaling (DWS)**
- **In-band TCP health checking:** Ability to determine the health of a server based on Layer 4 TCP analysis of application traffic between ACE and the backend server.
- **Cipher-based load balancing:** Distribution of application traffic based on the SSL cipher information.
- **Cookie strings:** Efficient HTTP sticky load balancing through the ability to set cookie value in the HTTP response from server to client.
- **KAL-AP enhancements:** Improved global application availability through KAL-AP enhancements in global server load balancing (GSLB).
- **Probe port inheritance:** Greatly simplifies the configuration for probes, especially in large-scale environment supporting multiple services per server.
- **Cisco TelePresence® audit trail support:** Syslogs for Session Initiation Protocol (SIP) load balancing have been added for Cisco ACE integration with Cisco TelePresence solutions.

Table 2 details the new features available on the Cisco ACE30 module running Cisco ACE Software Release A5(1.x). Table 3 lists the new features on the Cisco ACE30 module running Cisco ACE Software Release A4(2.x). Both tables provide comparisons to the Cisco ACE10 or ACE20 module running Cisco ACE Software Release A2(3.x).

Table 2. New Features on the Cisco ACE30 Module Running Cisco ACE Software Release A5.1.x

Feature	Description	Benefit
IPv6 SLB and baseline features	All of the current capabilities on the Cisco ACE platforms, including load-balancing and context-switching capabilities are now expanded to work in an IPv6 network. This includes support for (but is not limited to): • IPv6 interfaces, virtual IPs (VIPs) and server-farms • IPv6-based predictors and persistence • IPv6-based probes for health monitoring • IPv6-based Source NAT and extended access control lists (ACLs) • IPv6-based static routes • Virtualization • SSL including Client Certificate Authentication • CLI support for IPv6	Extends all current L4-L7 capabilities on the ACE platforms to work in an IPv6-enabled network.
Dual-Stack IPv4/IPv6 implementation	A dual-stack approach to IPv6 enables the Cisco ACE to support both IPv4-to-IPv4 and IPv6-to-IPv6 load-balancing. It also provides support for IPv6 to IPv4 translation (bi-directional) All deployment models (one-arm, routed, bridge mode, NAT, direct server return (DSR)) are supported with minimal loss of performance for IPv4 traffic.	Allows customers to gradually transition their networks to IPv6 as demand for IPv6 increases.
IPv6 protocol Support	The protocols supported by the Cisco ACE in an IPv6 network environment include HTTP, HTTPS and SSL.	Provides load-balancing and context switching capabilities for all web applications running in an IPv6 network.
IPv6 management	End-to-end IPv6 management (including provisioning, monitoring and troubleshooting) is supported by the following: • The Cisco Application Networking Manager (ANM) 5.1 via an intuitive web-based GUI interface. • The Device Manager (DM) on the Cisco ACE 4710 appliance via a web-based GUI interface and the ACE XML interface	Allows provisioning and end-to-end management of the solution through easy-to-use GUI-based tools.
IPv6 certification	IPv6 implementation on the Cisco ACE platforms is compliant with: • USGv6 certification • IPv6 Ready Logo Phase 2 certification	Meets certification requirements of Federal/government agencies.
Online Certificate Status Protocol (OCSP) support	This includes RFC2560 compliant support for OCSP. Up to 64 OCSP servers can be configured on the device in addition to mechanism to extract OCSP server information from the certificate itself. Use of OCSP does not preclude use of current CRL functionality.	Saves the ACE control plane from compute intensive certificate revocation validation processing and caching of Certificate Revocation Lists (CRLs).

Table 3. New Features on the Cisco ACE30 Module Running Cisco ACE Software Release 4.2.x

Feature	Description	Benefit
HTTP compression	The Cisco ACE30 module can compress the data being downloaded from the back-end server to the client browser. The compression algorithms supported are ZIP, GZIP, and Deflate. The maximum throughput for compression is 6 Gbps.	Reduces the WAN bandwidth consumption, leading to cost savings and faster download times.
In-Band TCP health checking	The Cisco ACE30 module can check the health of an application server before forwarding traffic to it by using the TCP Layer 4 responses from the application server.	Enables more connections to be set up per second because there are no separate health check probes; hence it can serve a higher rate of incoming connections.
Cipher-based load balancing	The Cisco ACE30 module can make load balancing decisions based on the specific SSL cipher or cipher strength used to initiate an SSL session.	Enables traffic distribution to separate server pools based on the SSL encryption method.

Feature	Description	Benefit
Cookie value specification	The Cisco ACE30 module can enter a cookie string value of the real server for HTTP cookie insertion when establishing a sticky connection. With this feature enabled, the Cisco ACE inserts the cookie in the Set-Cookie header of the response from the server to the client.	Enables intelligent web serving with stickiness of the same client to the same real server using server-side information.
KAL-AP enhancements	The Cisco ACE30 module uses this enhancement in global server load balancing, through which the Cisco Global Site Selector (GSS) reports the correct state of a failed Cisco ACE30 module in the Domain Name System (DNS) response to the client if a redundant Cisco ACE is present in a secondary data center.	Reduces application downtime for end users for a globally load-balanced application due to failure of the primary Cisco ACE in a distributed cluster of Cisco ACE load balancers (one or more in each global site).
Probe port Inheritance	The Cisco ACE30 module can dynamically inherit the port number for a probe from the real server specified in a server farm or from the virtual IP address specified in a Layer 3 or 4 class map.	Provides ease of configuration for probing real servers; only a single probe configuration is sufficient to probe a real server on multiple ports or on all virtual IP ports.
Syslog reporting for SIP load balancing	The Cisco ACE30 module can report the Layer 7 processing status for SIP packets as well as the reason for dropping any SIP packet during Layer 7 processing.	Enables the service provider or enterprise IT operator to troubleshoot SIP-based communication.

Detailed CLI Changes Between the Cisco ACE Software Release A2.3.x and A5.1.x

The vast majority of features and commands on the Cisco ACE modules are the same, however in the development of the Cisco ACE30 module some commands were modified to extend their functionality. Table 4, is a comprehensive list of all Cisco ACE10 or ACE20 commands that have been modified in Cisco ACE30. This table lists the command, an example of how it is used, and a brief description of the new command. Please take a moment to familiarize yourself with the minor changes listed.

Table 4. Modified ACE 2.x Commands

Command Syntax and Example	Description
`syn-cookie <value>` `This cli under interface configuration is modified for values < 4 to autoupgrade the values to 4.`	syn-cookie configuration.
`show ft group status` `itasca2/Admin# show ft group status` `FT Group : 1` `Configured Status : in-service` `Maintenance mode : MAINT_MODE_OFF` `My State : FSM_FT_STATE_ACTIVE` `Peer State : FSM FT STATE STANDBY BULK` `Peer Id : 1` `No. of Contexts : 1` `Running cfg sync status : Config sync disabled when peer is not fully CLI compatible` `Startup cfg sync status : Config sync disabled when peer is not fully CLI compatible`	Adding two “running/startup config sync status” entries in the end.
`show ft group brief` `itasca2/Admin# show ft group br` `FT Group ID: 1` `My State:FSM_FT_STATE_ACTIVE` `Peer State:FSM_FT_STATE_STANDBY_BULK` `Context Name: Admin` `Context Id: 0` `Cfg Sync Status:Successful`	Adding “cfg sync status” entry in the end.

Command Syntax and Example	Description
failaction reassign **<across-if>** switch/Admin(config-sfarm-host)#failaction reassign **across-if**	across-interface option added for failaction reassign.
show np <num> mtrie dest-ip <ip> switch/Admin# sh np 1 mtrie dest 1.1.1.1 level 0 Mnode found, next index=1. Search terminating successfully, Leaf found. ip resolve flag 0, ecmp flag 0, nat flag 0 Route/ECMP result #1 encaps id 0 if id 0 CHange only applicable for NAT entries	Change accounting octeons.
License uninstall [all | ?] switch/Admin# license uninstall all	'All' token and command completion is newly added.
show kalap udp load tag <tag name> show kalap udp load vip tag <tag name> VIP Tag Name VIP Port Load Value Time Last Updated	Show kalap tag command.
[no] crypto crlparams <crlName> cacert <CACertFileName> DM2/Admin(config)# crypto crlparams crl1 cacert cacert1.pem	CrlParams config command.
no]crypto crl <crlName> ldap://<hostNameOrIPAdress>/<DNName>[?certificateRevocationList][?one|base|sub][?objectclass=<filter>] DM2/Admin(config)# crypto crl crlLdap ldap://10.7.107.122:389/cn=Visa Systems,o=Verisign,c=us?certificateRevocationList	LDAP Url based Crl Config.
crypto import bulk sftp passphrase [non-exportable] pasphrase <passphrase> <host ip address> <user name> <remote path with wild card> DM2/Admin# crypto import bulk sftp passphrase ABCD 10.1.1.1 root /root/srccryptodir/*	Bulk import of crypto files.

New ACE Commands (Not Including IPv6)

The Cisco ACE30 module adds a variety of features and functionality to the Cisco ACE portfolio. Table 5 provides an extensive list of the new CLI commands for configuring the new Cisco ACE30 functionality, except for the IPv6 commands. In the Cisco ACE Software Release A5.1.0, IPv6 support was introduced to the Cisco ACE product line, but due to the number of IPv6 commands they have been omitted from Table 5. Please see the Cisco ACE documentation set for details on configuring IPv6 on the Cisco ACE30 module.

Table 5. New ACE Commands

Command Syntax and Example	Description
[no] cdp-errors ignore parameter-map type ssl SSL_PMAP cdp-errors ignore	Added cdp-errors ignored to ssl parammap
crl srvrcrl ssl-proxy service SSL_CLIENT authgroup simple crl srvrcrl	Enable CRL configuration for backend ssl

Command Syntax and Example	Description
[no] authentication-failure { ignore | redirect reason serverfarm | URL_string 301|302} parameter-map type ssl test_ssl_pmap authentication-failure redirect any url http://www.cisco.com/ 301	Currently if an SSL handshake fails because of a problem such as a bad client certificate, the default action is for ACE to terminate the handshake. The behavior can be changed to allow such connections via the "authentication-failure ignore" flag in the SSL parameter map.
[no] rehandshake enabled parameter-map type ssl rehdshake rehandshake enabled	By default, rehandshake is disallowed for both front-end and back-end SSL on ACE. Allowing rehandshake by adding this parameter map.
[no] switch-mode ACE30-slot3/Admin# conf t Enter configuration commands, one per line. End with CNTL/Z. ACE30-slot3/Admin(config)# switch-mode ACE30-slot3/Admin(config)# no switch-mode	Enables switch-mode in context.
1.[no] ip address <ip> <mask> secondary 2. [no] peer ip address <ip> <mask> secondary 3. [no] alias <ip> <mask> secondary interface vlan 3000 ip address 4.3.2.1 255.255.255.0 ip address 10.2.0.54 255.255.255.0 secondary peer ip address 10.2.0.53 255.255.255.0 secondary alias 10.2.0.55 255.255.255.0 secondary service-policy input MGMT no shutdown	Allows configuration of secondary addresses under an interface.
[no] inband-health check { count | { log <fail-threshold count> } | { remove <fail-threshold count> [resume-service <seconds>] } } ACE30/Admin(config-sfarm-host)# inband-health check count ACE30/Admin(config-sfarm-host)# inband-health check log 2 ACE30/Admin(config-sfarm-host)# inband-health check remove 4 ACE30/Admin(config-sfarm-host)# inband-health check remove 20 resume-service 300 ACE30/Admin(config-sfarm-host)#no inband-health	Command to configure inband HM
failaction reassign **<across-if>** switch/Admin(config-sfarm-host)#failaction reassign **across-if**	across-interface option added for failaction reassign
[no] header insert { both | request | response} <header-name> header-value <header-value> action-list type modify http TEMP header insert both HEADER_NAME_STR header-value "HEADER_VALUE_STR"	A HTTP header name/value pair will be inserted in request, response or both
backup {all | exclude <exclude-str>| passphrase <passphrase>} switch/Admin# backup pass-phrase df exclude checkpoints Backup started. Use show commands for status information.	Secure backup/restore feature
Restore {all | disk0:<archive-name>} [exclude <ssl-file> | passphrase <passphrase>] switch/Admin# restore al disk0:switch_Admin_2010_03_05_05_44_08.tgz pass-phrase ad Error: Passphrase incorrect. Archive restore failed. switch/Admin# restore al disk0:switch Admin 2010 03 05 05 44 08.tgz pass-phrase df Restore started. Use show commands for status information.	Secure backup/restore feature

Command Syntax and Example	Description
[no] kal-ap-tag <tag name> switch/Admin(config)# policy-map multi-match l3 class vip loadbalance policy l7 loadbalance vip inservice kal-ap-tag abc	Configures kalap tag name
KAL-AP-TAG213 92.0.1.13 eq 80 0 Tue Dec 16 08:34:41	Show command for kalap tag
[no]crypto crl <crlName> ldap://<hostNameOrIPAdress>/<DNName>[?certificateRevocationList][?one|base|sub][?objectclass=<filter>] DM2/Admin(config)# crypto crl crlLdap ldap://10.7.107.122:389/cn=Visa Systems,o=Verisign,c=us?certificateRevocationList	LDAP URL based CRL Config.
crypto import bulk sftp passphrase [non-exportable] pasphrase <passphrase> <host ip address> <user name> <remote path with wild card> DM2/Admin# crypto import bulk sftp passphrase ABCD 10.1.1.1 root /root/srccryptodir/*	Bulk import of crypto files.
reverse-sticky STICKY-GROUP-NAME (Of type Ip sticky.) switch/ACE2(config)# policy-map type loadbalance first-match L7PMAP switch/ACE2(config-pmap-lb)# switch/ACE2(config-pmap-lb)# class class-default switch/ACE2(config-pmap-lb-c)# reverse-sticky ? <WORD> Enter sticky group name (Max Size - 64) DEST_IP_STICKY DEST IP STICKY1 DEST IP STICKY2 DEST IP STICKY3 DEST_IP_STICKY4 DEST_IP_STICKY5	Configure a sticky group as a reverse sticky one.
[no] kal-ap primary-oos policy-map multi-match L7LB class VIP loadbalance vip inservice loadbalance policy HTTP_POLICY loadbalance vip icmp-reply kal-ap primary-oos	Configures kal-ap primary-oos Setting the configuration command “kal-ap primary-oos”, when the primary serverfarm is down and VIP is in inservice state due to back-up serverfarm taking over, the load value for VIP is set to KALAP_OVERLOADED to ensure all the subsequent DNS requests are redirected
[no] logging all parameter-map type sip sip_param logging all	A SIP parameter map configuration to configure SIP inspect engine to generate syslogs for received and transmitted SIP packets.
clear dc <0|1> controller stats switch/Admin# clear dc 1 controller stats	Clears the data plane (verni) statistic registers
set dc <0|1> console <master|slave> switch/Admin# set dc 0 console slave Switched the console access to slave octeon	Switch the console access to master or slave

Command Syntax and Example	Description
system watchdog memory [timeout] switch/Admin# show system watchdog ? lcp Show LCP watchdog status memory Show watchdog memory status scp Show SCP watchdog status | Output modifiers. > Output Redirection. <cr> Carriage return. switch/Admin# show system watchdog LCP watchdog : Enabled Timeout: 20 seconds SCP watchdog : Enabled Timeout: 13 seconds Memory watchdog : Enabled Timeout: 90 seconds switch/Admin# system no watchdog memory Disabling low Memory Watchdog switch/Admin# system no watchdog lcp Disabling LCP Watchdog switch/Admin# system no watchdog scp Disabling SCP Watchdog switch/Admin# show system watchdog LCP watchdog : Disabled SCP watchdog : Disabled Memory watchdog : Disabled	

New ACE show Commands

The Cisco ACE30 module also adds numerous **show** commands to aid in the operation and administration of the Cisco ACE30 module. Table 6, provides a detailed list of the new CLI **show** commands. This table lists the command, an example of how it is used, and a brief description of the new command. For IPv6 specific show commands, please see the Cisco ACE documentation set for details on configuring IPv6 on the Cisco ACE30 module.

Table 6. New ACE Show command and output

Command Syntax and Example	Description
show dc <0|1> controller all switch/Admin# show dc 0 controller all SNO Verni Register Name Address Value 0 VERNI_FPGA_REV_REG_ADDR 0x 0 0x20104 1 VERNI_FIFO32RXDYNPSREG_REG_ADDR 0x 4 0x80 2 VERNI CFG REG ADDR 0x 10 0x1601 3 VERNI CFG OTN REG ADDR 0x 1c 0x0 4 VERNI STS REG ADDR 0x 18 0x17f 5 VERNI TEST REG ADDR 0x 20 0x0 6 VERNI LED CTRL REG ADDR 0x 30 0xf 7 VERNI_PERR_REG_ADDR 0x 70 0x0 8 VERNI_FPERR_REG_ADDR 0x 74 0x0 9 VERNI_O_ISR_REG_ADDR 0x 100 0xc60000 10 VERNI O IER REG ADDR 0x 104 0x0 11 VERNI O IIR REG ADDR 0x 108 0x0 12 VERNI S ISR REG ADDR 0x 200 0x0 13 VERNI S IER REG ADDR 0x 204 0x0 14 VERNI S IIR REG ADDR 0x 208 0x0 15 VERNI_OM_STS_REG_ADDR 0x1000 0x8 16 VERNI_OM_IER_REG_ADDR 0x1004 0x0	Dumps all data plane (aka verni) register.
show dc <0|1> console switch/Admin# show dc 0 console mCPU console is directed to base board front panel	Displays whether the master or slave CPU is directed to base board front panel.

Command Syntax and Example	Description
show dc <0|1> controller reg <0x0000-0x7fff> switch/Admin# show dc 0 controller reg 0x0000 Register Name : VERNI FPGA REV REG ADDR Description : Verni FPGA Revision Register Value : 0x20104 Register Type : General Register	Dumps the value, type, and description of the register given
show dc <0|1> controller stats <cumulative|delta> 0 VERNI_CSR_CNTL_REG_ADDR 0x 80 0x0 1 VERNI_DCRX0_BYTCNT_H_REG_ADDR 0x3100 0x0 2 VERNI DCRX0 BYTCNT L REG ADDR 0x3104 0x0 3 VERNI DCRX1 BYTCNT H REG ADDR 0x3110 0x0 4 VERNI DCRX1 BYTCNT L REG ADDR 0x3114 0x1365e 5 VERNI DCRX2 BYTCNT H REG ADDR 0x3120 0x0 6 VERNI DCRX2 BYTCNT L REG ADDR 0x3124 0xf23 7 VERNI_DCRX3_BYTCNT_H_REG_ADDR 0x3130 0x0 8 VERNI_DCRX3_BYTCNT_L_REG_ADDR 0x3134 0x0 9 VERNI_DCRX4_BYTCNT_H_REG_ADDR 0x3140 0x0 10 VERNI DCRX4 BYTCNT L REG ADDR 0x3144 0x0 11 VERNI DCRX5 BYTCNT H REG ADDR 0x3150 0x0 12 VERNI DCRX5 BYTCNT L REG ADDR 0x3154 0x13238 13 VERNI DCRX6 BYTCNT H REG ADDR 0x3160 0x0 14 VERNI_DCRX6_BYTCNT_L_REG_ADDR 0x3164 0x0 15 VERNI_DCRX7_BYTCNT_H_REG_ADDR 0x3170 0x0 16 VERNI_DCRX7_BYTCNT_L_REG_ADDR 0x3174 0x0 17 VERNI DCRX0 PKTCNT REG ADDR 0x3200 0x0 18 VERNI_DCRX1_PKTCNT_REG_ADDR 0x3204 0x2fbf	Dumps all the stats register
show dc <0|1> controller health switch/Admin# sh dc 1 controller health Tnrpc call for INFO_VERN_REGISTERS Success CDE<->Verni FIFO Interface: Cumulative Delta --- DC RX Channel status: Healthy DC Rx bytes received : 57014 26511 DC Rx packets received : 1229 115 DC Rx error packets received : 0 0 DC Rx flow control events : 0 0 DC Rx dropped packets : 0 0 DC Tx bytes transmitted : 38470 10782 DC Tx packets transmitted : 453 115 DC Tx error packets : 0 0 DC Tx crc error packets : 0 0 Verni <-> Octeon SPI4.2 Interface --- Sink Channel Status : Healthy Sink octets received : 38470 10782 Sink pass packets received : 453 115 Sink error packets received : 0 0 Sink generic errors received : 0 0 Source Channel Status : Healthy	Dumps data plane (aka verni) health

Command Syntax and Example	Description
Source bytes transmitted: 57014 26511 Source pass packets transmitted : 461 115 Source error packets transmitted : 0 0	
show dc <0|1> controller interrupts sjc-itasca-ssl-fusion/Admin# sh dc 1 controller interrupts DC Interrupt Status (0x200) ------------------------------ Incorrect queue mapping to Tx Channel 7 0 Incorrect queue mapping to Tx Channel 6 0 Incorrect queue mapping to Tx Channel 5 0 Incorrect queue mapping to Tx Channel 4 0 Incorrect queue mapping to Tx Channel 3 0 Incorrect queue mapping to Tx Channel 2 0 Incorrect queue mapping to Tx Channel 1 0 Incorrect queue mapping to Tx Channel 0 0 Quack interface interrupt 0 Internal BRAM parity error 0 Itasca CSR bus write parity error 0 Itasca mailbox access error 0 Mailbox doorbell from Octeon interrupt 0 Mailbox acknowledge from the Octeon interrupt 0 Octeon Spi4.2 Sink interface per channel error 0 Octeon Spi4.2 Sink interface general error 0 Octeon Spi4.2 Source interface error 0 Daughter card Rx interface channel 7 error 0 Daughter card Rx interface channel 6 error 0 Daughter card Rx interface channel 5 error 0 Daughter card Rx interface channel 4 error 0 Daughter card Rx interface channel 3 error 0 Daughter card Rx interface channel 2 error 0 Daughter card Rx interface channel 1 error 0 Daughter card Rx interface channel 0 error 0	Dumps all data plane (aka verni) interrupt register
show service-policy url-summary switch/Admin# sh service-policy url-summary Service-Policy: L3 L3-Class: vip L7-Class: L7 match http url /index.html hit: 4 Service-Policy: L3 L3-Class: vip1 L7-Class: L7 match http url /index.html hit: 4	Dumps the Layer7 URLs configured along with hit counter, under Layer7 policy referenced by multi-match policy.
sh service-policy <policy-name> url-summary switch/Admin# sh service-policy L3 url-summary Service-Policy: L3 L3-Class: vip L7-Class: L7 match http url /index.html hit: 18 Service-Policy: L3 L3-Class: vip1 L7-Class: L7 match http url /index.html hit: 18	Dumps the Layer7 URLs configured along with hit counter, under Layer7 policy referenced by multi-match policy.
sh service-policy <policy_name> class-map <class-name> url-summary switch/Admin# sh service-policy slb class-map vip url-summary Service-Policy: slb L3-Class: vip L7-Class: L7 class match http url /index.html hit: 0	Dumps the Layer7 URLs configured along with hit counter, under Layer7 policy referenced by multi-match policy.

Command Syntax and Example	Description
`show stats crypto server insert` `switch/Admin# show stats crypto server redirect` `Session headers extracted: 0` `Session headers failed: 0` `Server cert headers extracted: 0` `Server cert headers failed: 0` `Client cert headers extracted: 0` `Client cert headers failed: 0` `Headers truncated: 0` `Header insert buffer limit hit: 0`	Added subtype for new header insert stats
`show stats crypto server redirect` `switch/Admin# show stats crypto server insert` `Redirects due to cert not yet valid: 0` `Redirects due to cert expired: 0` `Redirects due to unknown issuer cert: 0` `Redirects due to cert revoked: 0` `Redirects due to no client cert: 0` `Redirects due to no CRL available: 0` `Redirects due to expired CRL: 0` `Redirects due to bad cert signature: 0` `Redirects due to other cert error: 0`	Added subtype for new redirect stats
`show hardware` `ACE30/Admin# show hardware` `Hardware` `Product Number: ACE30-MOD-K9` `Serial Number: SAL1413E2YN` `Card Index: 207` `Hardware Rev: 0.101` `Feature Bits: 0000 0004` `Slot No. : 1` `Type: ACE` `Daughter Card` `Product Number: ACEMOD-EXPN-DC` `Serial Number: SAL1413ECLJ` `Card Index: 309` `Hardware Rev: 0.602` `Feature Bits: 0000 0001` `Slot No. : 1` `Controller FPGA Rev:1.5` `NP 1:` `Clock Rate: 600000000 Hz` `Memory Size: 4096 MB` `NP 2:` `Clock Rate: 600000000 Hz` `Memory Size: 4096 MB` `Daughter Card` `Product Number: ACEMOD-EXPN-DC` `Serial Number: SAL1413ECKM` `Card Index: 309`	Added data plane (aka verni) revision details in the show hardware output

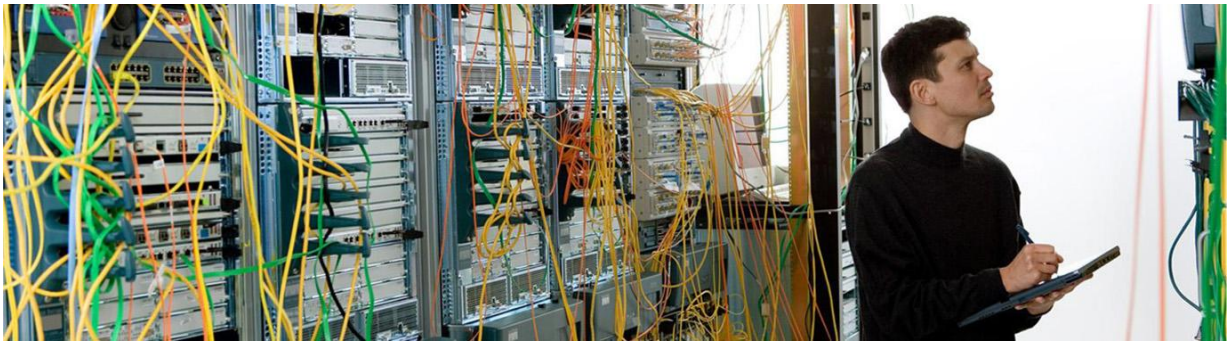
Command Syntax and Example	Description
Hardware Rev: 0.602 Feature Bits: 0000 0001 Slot No. : 2 Controller FPGA Rev:1.5 NP 3: Clock Rate: 600000000 Hz Memory Size: 4096 MB NP 4: Clock Rate: 600000000 Hz Memory Size: 4096 MB	
show crypto cdp-errors avneet-scim-4/Admin# sh crypto cdp-errors Incomplete: 0 Malformed: 0 Unrecognized Transports: 0 Missing from cert: 0 Best Effort CDP Errors Ignored: 0	Added Best Effort CDP Errors Ignored stats
1. show resource usage np <1|2|3|4> [all|context name| summary] 2. show resource usage np <current| peak|denied> [all|context name| summary]	Show command
Show download Information <summary | all> switch/Admin# show download information context : Admin Interface Download-status ---------- 501 Completed 50 Completed 398 Completed 551 In Progress 560 Pending switch/Admin# sh download information context : Admin Interface Download-status ---------- 501 Completed 50 Pending/Deleted 398 Completed 551 Pending 560 Pending/Deleted	Displays the download information with granularity at interface level
show acl-merge event-history switch/Admin# sh acl-merge event-history 1) Event:E DEBUG, length:81, at 267829 usecs after Mon Jan 4 02:37:19 2010 [104] <Ctx:3>< >ACL-MERGE acl_merge_create_merged_list START: instance:12 context:3 2) Event:E DEBUG, length:81, at 267232 usecs after Mon Jan 4 02:37:19 2010 [104] <Ctx:3>< >ACL-MERGE acl merge create merged list START: instance:11 context:3	

Command Syntax and Example	Description
show/clear serverfarm <name> inband ACE30/Admin# show serverfarm web inband serverfarm : web rserver : lnx1[0] action : remove Total Delta ---------- SYN RSTs : 0 0 SYN Timeouts : 0 0 ICMP Network Unreachable : 0 0 ICMP Host Unreachable : 0 0 ICMP Port Unreachable : 0 0 ICMP Protocol Unreachable : 0 0 ICMP Source Route Failed : 0 0	Command to show inband stats
show ft group status itasca2/Admin# show ft group status FT Group : 1 Configured Status : in-service Maintenance mode : MAINT MODE OFF My State : FSM_FT_STATE_ACTIVE Peer State : FSM_FT_STATE_STANDBY_BULK Peer Id : 1 No. of Contexts : 1 Running cfg sync status : Config sync disabled when peer is not fully CLI compatible Startup cfg sync status : Config sync disabled when peer is not fully CLI compatible	Adding two “running/startup config sync status” entries in the end
show ft group brief itasca2/Admin# show ft group br FT Group ID: 1 My State:FSM FT STATE ACTIVE Peer State:FSM FT STATE STANDBY BULK Context Name: Admin Context Id: 0 Cfg Sync Status:Successful	Adding “cfg sync status” entry in the end
show backup status [detail] switch/Admin# sh backup status Backup Archive: switch Admin 2011 05 19 05 03 55.tgz Type : Context Start-time : Thu May 19 05:03:55 2011 Finished-time : Thu May 19 05:03:55 2011 Status : SUCCESS Current vc : Admin Completed : 1/1 switch/Admin# sh backup status de Backup Archive: switch Admin 2011 05 19 05 03 55.tgz Type : Context Start-time : Thu May 19 05:03:55 2011 Finished-time : Thu May 19 05:03:55 2011 Status : SUCCESS Current vc : Admin Completed : 1/1 ========== Context component Time Status	New CLI for secure backup/restore feature

Command Syntax and Example	Description
`` ========== Admin Running-cfg Thu May 19 05:03:55 2011 SUCCESS Admin Startup-cfg Thu May 19 05:03:55 2011 SUCCESS Admin Checkpoints Thu May 19 05:03:55 2011 SUCCESS Admin Cert/Key Thu May 19 05:03:55 2011 SUCCESS Admin License Thu May 19 05:03:55 2011 SUCCESS Admin Probe script Thu May 19 05:03:55 2011 SUCCESS ```	
`` show restore status [detail] switch/Admin# sh restore status Backup Archive: switch Admin 2011 05 19 05 08 39.tgz Type : Context Start-time : Thu May 19 05:09:14 2011 Finished-time : - Status : In Progress Current vc : Admin Completed : 0/1 switch/Admin# sh restore status de Backup Archive: switch Admin 2011 05 19 05 08 39.tgz Type : Context Start-time : Thu May 19 05:09:14 2011 Finished-time : Thu May 19 05:09:25 2011 Status : SUCCESS Current vc : Admin Completed : 1/1 ========== Context component Time Status ========== Admin License Thu May 19 05:09:24 2011 SUCCESS Admin Cert/Key Thu May 19 05:09:24 2011 N/A Admin Probe script Thu May 19 05:09:24 2011 N/A Admin Checkpoints Thu May 19 05:09:24 2011 N/A Admin Startup-cfg Thu May 19 05:09:24 2011 N/A Admin Running-cfg Thu May 19 05:09:25 2011 SUCCESS ```	new CLI for secure backup/restore feature
`` show backup/restore errors switch/Admin# sh restore error Context: Admin component: running-config below diff couldn’t be applied. --- script 1 abcd.scr --- ```	Secure backup/restore feature
`` show kalap udp load tag <tag name> show kalap udp load vip tag <tag name> VIP Tag Name VIP Port Load Value Time Last Updated ```	Show kalap tag command
`` sh cfgmgr internal table rserver ACE30/revSticky# sh cfgmgr internal table rserver Rserver-id Rserver-Name Ctx Id Encap Flags 7 fw1 1 8 ADDED, UPDATED, RELOADED, DATA VALID, 8 fw2 1 9 ADDED, UPDATED, RELOADED, DATA_VALID, 9 rs1 1 7 ADDED, UPDATED, RELOADED, DATA_VALID, ```	Included a field for rserver encaps Id
sh stats sticky ``` ACE30/Admin# sh stats sticky +----------+ +---------- Sticky statistics ----------+ +----------+ Total sticky entries reused : 0 ```	Added two extra fields to the output for reverse sticky entries and global pool

Command Syntax and Example	Description
prior to expiry Total active sticky entries : 0 Total active reverse sticky entries : 0 Total active sticky conns : 0 Total static sticky entries : 0 Total sticky entries from Global Pool : 0 Total insertion failures due to lack of resources : 0	

Cisco ACE Migration Worksheet



Prerequisite Confirmation

Timeframe

The maintenance window for the Cisco ACE migration is on:_____ **(Date)**

The duration for the Cisco ACE migration maintenance window is: ____ hours **(Minimum 1 hour recommended)**

Staging Area

Where will the Cisco ACE30 modules be staged? _____

What is the IP address or console information for the Cisco Supervisor Engine 720 in the staging area? _____

What are the remote access credentials? username:_____ password: _____

Cisco IOS Software Release Verification

What is the current Cisco IOS Software Release in the staging area?_____

What is the current Cisco IOS Software Release in the production area? _____

The minimum requirements are as follows:

- Catalyst 6500 Sup720 Cisco IOS Software Release 12.2(33)SXI4 (or later)
- Catalyst 7600 Sup720 Cisco IOS Software Release 15.0(1)S (or later)
- Catalyst 7600 RSP720 Cisco IOS Software Release 15.0(1)S (or later)

Backup Server Connectivity

What is the IP address of the FTP/SFTP server where the backup file for the Cisco ACE10 or ACE20 modules will be kept? _____

Verify the server IP is reachable from the Cisco ACE30 modules while they are in the staging area: ☐ **yes**

Nonexportable SSL files

Do the production Cisco ACE10 or ACE20 modules use nonexportable SSL files? ☐ **yes** or ☐ **no**

If yes, will SSL backup files be imported, or will the SSL files be recreated? ☐ **imported** ☐ **recreated**

IP address and credentials for the SSL backup files: _____

ACE Licensing

Does the Cisco ACE30 module have a license file? ☐ Base Only ☐ 4G ☐ 8G ☐ 16G

Provide the location of the ACE license: _____

Fault-Tolerant Preemption

Is "no preemption" applied to all FT groups? (**show run ft**) ☐ ***yes*** or ☐ ***no***

List the FT groups that **do not** have "no preemption" configured: _____

_____

Are all contexts active on the primary ACE in production? (**show ft group brief**) ☐ **yes** or ☐ **no**

List the FT group IDs that **are not** active on the primary ACE in production: _____

_____

Staging the Cisco ACE30 Modules

Do not proceed until the staging area Sup720 is running the minimum required IOS Software Release for the Cisco ACE30 module.

Backups and Code Download

Step 1. Using the CLI or ANM, back up the active and standby Cisco ACE10 or ACE20 modules:

```
ACE-pri/Admin# backup all
ACE-pri/Admin# show backup status
```

Step 2. Export the backup files to a FTP/SFTP server. The Cisco ACE30s in staging must be able to reach the FTP or SFTP server to restore the configurations:

```
ACE-pri/Admin# copy backup-all sftp://172.25.91.127


ACE-sec/Admin# copy backup-all sftp://172.25.91.127
```

Step 3. Download the A4.2.1a version of the Cisco ACE image from Cisco.com.

http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Application+Control+Software&mdfid=280557289&treeName=Cisco+Interfaces+and+Modules&mdfLevel=SERIES&url=null&modelName=Cisco+ACE+Application+Control+Engine+Module&isPlatform=N&treeMdfId=268437717&modifmdfid=null&imname=&hybrid=Y&imst=N

Stage ACE30a (will be the primary)

Step 1. Physically install a new Cisco ACE30 module into Cisco Catalyst 6500 chassis in the staging area. This Cisco ACE30 module will be known as “ACE30a” henceforth.

Step 2. Install the A4.2.1a Cisco ACE Software image on Cisco ACE30a:

```
switch/Admin# copy sftp://172.25.91.127 image:
```

Step 3. Log into the ACE from the Sup720 and configure an interface and IP address to allow the ACE to connect to the backup server where the ACE20 backup files were stored in the preceding staging steps. If needed, add the appropriate default route to access backup servers if they are a hop away. Note: Neither ACLs nor management policies need to be configured as the ACE will initialize the outgoing connections in the staging process.

Step 4. Restore the backup of the primary ACE10 or ACE20 to ACE30a. Disregard the warning about the licensing file.

```
switch/Admin# copy sftp://172.25.91.127 disk0:
switch/Admin# restore all disk0:20a-primary.tgz
ACE-pri/Admin# show restore status
```

Step 5. Install a bandwidth license for the Cisco ACE 30 modules if applicable.

```
ACE30/Admin# copy <license_file_location_from_worksheet> disk0:
Enter source filename[]? ACE30-MOD-16-K9.lic
ACE30/Admin# license install disk0:ACE30-MOD-16-K9.lic
```

Step 6. Modify the boot string to load the Cisco ACE A4.2.1a Software image.

```
ACE-pri/Admin# show run | inc boot
ACE-pri/Admin(config)# boot system image:c6ace-t1k9-mz.A4_2_1a.bin
ACE-pri/Admin(config)# no boot system image:c6ace-t1k9-mz.<version>.bin
```

Step 7. Create a checkpoint of the ACE configuration, so that it can be restored after the production environment is migrated to the Cisco ACE30 modules.

```
ACE-pri/Admin# checkpoint create cfg-preempt
```

Step 8. If the Admin context has **preempt** configured within the FT groups, it must be removed to allow manual context failover and to prevent a premature failover during the migration. Edit the FT groups listed above in the worksheet so that all FT groups have **no preempt** configured.

```
ACE-pri/Admin# show run ft
```

Step 9. Save the ACE configuration and reload the Cisco ACE30 module to ensure it boots the new image as expected.

```
ACE-pri/Admin# wr mem all
ACE-pri/Admin# reload
```

Stage ACE30b (backup to be)

Step 1. Physically install a new Cisco ACE30 modules into Cisco Catalyst 6500 chassis in the staging area. This Cisco ACE30 module will be known as “ACE30b” henceforth.

Step 2. Install the A4.2.1a Cisco ACE Software image on ACE30b

```
switch/Admin# copy sftp://172.25.91.127 image:
```

Step 3. Log into the ACE from the Sup720 and configure an interface and IP address to allow the ACE to connect to the backup server where the ACE20 backup files were stored in the staging steps above. If needed add the appropriate default route to access backup servers if they are a hop away. Note: Neither ACLs nor Management policies need to be configured as the ACE will initiate the connections out in the staging process.

Step 4. Restore the backup of the primary ACE10 or ACE20 to ACE30b:

```
switch/Admin# copy sftp://172.25.91.127 disk0:
switch/Admin# restore all disk0:20b-secondary.tgz
ACE-sec/Admin# show restore status
```

Step 5. Install a bandwidth license for the Cisco ACE 30 modules if applicable:

```
ACE30/Admin# copy <license_file_location_from_worksheet> disk0:
Enter source filename[]? ACE30-MOD-16-K9.lic
ACE30/Admin# license install disk0:ACE30-MOD-16-K9.lic
```

Step 6. Modify boot string to load the A4.2.1a software image:

```
ACE-sec/Admin# show run | inc boot
ACE-sec/Admin(config)# boot system image:c6ace-t1k9-mz.A4_2_1a.bin
ACE-sec/Admin(config)# no boot system image:c6ace-t1k9-mz.A2_3_4.bin
```

Step 7. If the Admin context has **preempt** configured within the FT groups, it must be removed to allow manual context failover and to prevent a premature failover during the migration. Edit the FT groups listed above in the worksheet so that all FT groups have **no preempt** configured.

```
ACE-pri/Admin# show run ft
```

Step 8. Save the ACE configuration and reload the Cisco ACE30 module to ensure it boots the new image as expected.

```
ACE-sec/Admin# wr mem all
ACE-sec/Admin# reload
```

Migrating to the Cisco ACE30 Modules

Do not proceed until the production area Sup720 is running the minimum required Cisco IOS Software Release for the Cisco ACE30 module.

Migrate Backup ACE10 or ACE20 to ACE30

1. On the primary (active) Cisco ACE 10 or ACE20 module, create a checkpoint of the current configuration.

```
ACE-pri/Admin# checkpoint create pri-orig
```

2. If the Admin context on the primary Cisco ACE10 or ACE20 module has **preempt** configured within the FT groups, it must be removed to allow manual context failover and to prevent a premature failover during the migration process. Edit the FT groups listed above in the worksheet so that all FT groups have **no preempt** configured.

```
ACE-pri/Admin# show run ft
```

3. Power-down the backup ACE10 or ACE20 from the secondary Cisco Catalsyt Sup720:

```
cat6k-sec#show module services
cat6k-sec(config)#no power enable module 1
```

4. Physically replace the backup Cisco ACE10 or ACE20 module with the Cisco ACE30b module.
5. Power-on ACE30b. The ACE30b will boot as standby.

```
cat6k-sec(config)#power enable module 1
```

6. Once ACE30b is warm, perform the the ACE10 or ACE20 failover:

```
cat6k-sec#session s 1 p 0

ACE-sec /Admin# show ft group brief

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

7. Verify the FT group transition using the **show ft group brief** command. All the FT groups should show a My State as active and the Sync Status as Successful.

```
ACE-sec/Admin# show ft group brief
```

Migrate Primary ACE10 or ACE20 to ACE30

1. Power-down the primary ACE10 or ACE20 from the primary Cisco Catalsyt Sup720.

```
cat6k-pri#show module services
cat6k-pri(config)#no power enable module 1
```

2. Physically replace the primary Cisco ACE10 or ACE20 module with the Cisco ACE30a module.
3. Power on ACE30a. The ACE30a will boot as standby.

```
cat6k-pri(config)#power enable module 1
```

4. Once ACE30b is warm, perform the ACE30b failover:

```
cat6k-pri#session s 1 p 0

ACE-pri /Admin# show ft group brief

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

5. Verify the FT group transition using the **show ft group brief** command. All the FT groups should show a My State as active and the Sync Status as Successful.

```
ACE-pri/Admin# show ft group brief
```

6. Roll back the checkpooint created in the “Stage ACE30a” section to roll back the previous preemption settings in each FT group:

```
ACE-pri/Admin# checkpoint rollback cfg-preempt
```

7. Save the restored configuration, and the configurations for all other contexts:

```
ACE-pri/Admin# wr mem all
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C17-688041-00 10/11