This article describes the procedures for troubleshooting redundancy issues with your ACE.

Guide Contents
Main Article
Overview of ACE Troubleshooting
Understanding the ACE Module Architecture and Traffic Flow
Preliminary ACE Troubleshooting
Troubleshooting ACE Boot Issues
Troubleshooting with ACE Logging
Troubleshooting Connectivity
Troubleshooting ACE Appliance Ethernet Ports
Troubleshooting Remote Access
Troubleshooting Access Control Lists
Troubleshooting Network Address Translation
Troubleshooting ACE Health Monitoring
Troubleshooting Layer 4 Load Balancing
Troubleshooting Layer 7 Load Balancing
Troubleshooting Redundancy
Troubleshooting SSL
Troubleshooting Compression
Troubleshooting Performance Issues
ACE Resource Limits
Managing ACE Resources
Show Counter Reference

Contents

Overview of ACE Redundancy

Redundancy (or fault tolerance) allows your network to remain operational even if one of the ACEs becomes unresponsive. Redundancy ensures that your network services and applications are always available.

Redundancy provides seamless switchover of flows if an ACE becomes unresponsive or a critical host, interface, or HSRP group (ACE module only) fails. Redundancy supports the following network applications that require fault tolerance:

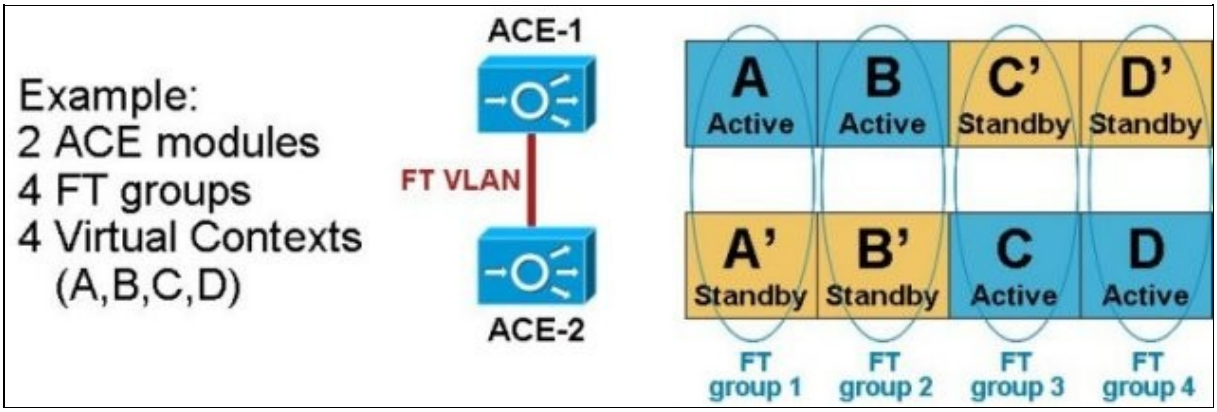
- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

Redundancy Protocol

You can configure a maximum of two ACE modules (peers) in the same Catalyst 6500 series switch or in different chassis for redundancy. You can also configure a maximum of two ACE 4710 appliances for redundancy. Each peer ACE can contain one or more fault-tolerant (FT) groups. Each FT group consists of two members: one active context and one standby context. For more information about contexts, see the *Cisco Application Control Engine Module Virtualization Configuration Guide* or the *Cisco 4700 Series Application Control Engine Appliance Administration Guide (Software Version A3(2.4))*. An FT group has a unique group ID that you assign.

Both ACEs can be active at the same time, processing traffic for distinct virtual devices and backing up each other (stateful redundancy). An Active-Active configuration requires two FT groups and two virtual contexts on each ACE. See Figure 1.

Figure 1. Example of an Active-Active Configuration



The ACE uses the redundancy protocol to communicate between the redundant peers. The election of the active member within each FT group is based on a priority scheme. The member configured with the higher priority is elected as the active member. If a member with a higher priority is found after the other member becomes active, the new member becomes active because it has a higher priority. This behavior is known as preemption and is enabled by default.

One virtual MAC address (VMAC) is associated with each FT group. The format of the VMAC is: 00-0b-fc-fe-1b-groupID. Because a VMAC does not change upon a switchover, the client and server ARP

tables does not require updating. The ACE selects a VMAC from a pool of virtual MACs available to it. You can specify the pool of MAC addresses that the local ACE and the peer ACE use by configuring the **shared-vlan-hostid** command and the **peer shared-vlan-hostid** command, respectively. To avoid MAC address conflicts, be sure that the two pools are different on the two ACEs. For more information about VMACs and MAC address pools, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

Each FT group acts as an independent redundancy instance. When a switchover occurs, the active member in the FT group becomes the standby member and the original standby member becomes the active member. A switchover can occur for the following reasons:

- The active member becomes unresponsive.
- A tracked host, interface, or HSRP group fails.
- You enter the **ft switchover** command to force a switchover.

FT VLAN

Redundancy uses a *dedicated* FT VLAN between redundant ACEs to transmit flow-state information and the redundancy heartbeat. You must configure this same VLAN on both peer ACEs. You also must configure a different IP address within the same subnet on each ACE for the FT VLAN. Cisco recommends two port-channeled 1-Gigabit Ethernet links for the FT VLAN. For the appliance, when you configure the **ft-port-vlan** command, the ACE modifies the associated Ethernet port or port-channel interface **to a trunk port**, so you have to put your switch port in trunk mode or tag the FT VLAN, it's very important.

Note: Do not use the FT VLAN for any other network traffic, including HSRP traffic and data.
The two redundant ACEs constantly communicate over the FT VLAN to determine the operating status of each ACE. The standby member uses the heartbeat packet to monitor the health of the active member. The active member uses the heartbeat packet to monitor the health of the standby member. Communications over the switchover link include the following data:

- Redundancy protocol packets
- State information replication data
- Configuration synchronization information
- Heartbeat packets

For multiple contexts, the FT VLAN resides in the system configuration file. Each FT VLAN on the ACE has one unique MAC address associated with it. The ACE uses these device MAC addresses as the source or destination MACs for sending or receiving redundancy protocol state and configuration replication packets.

Note: The IP address and the MAC address of the FT VLAN do not change at switchover.

Configuration Requirements and Restrictions

Follow these requirements and restrictions when configuring the redundancy feature:

- Redundancy is not supported between an ACE module and an ACE appliance operating as peers. Redundancy must be of the same ACE device type and software release.
- In bridged mode (Layer 2), two contexts cannot share the same VLAN.
- To achieve active-active redundancy, a minimum of two contexts and two FT groups are required on each ACE.
- When you configure redundancy, the ACE keeps all interfaces that do not have an IP address in the Down state. The IP address and the peer IP address that you assign to a VLAN interface should be in the same subnet but should be different IP addresses. For more information about configuring VLAN

interfaces, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide* or the *Cisco ACE 4700 Series Appliance Routing and Bridging Configuration Guide*

- FT Interfaces are put into an automatic **trunk status** and, for the module, the Catalyst 6500 series switch needs to be set to trunk the specific VLAN you are using for the FT interface.

Example of a Redundancy Configuration

The following example shows a running-configuration file that defines fault tolerance (FT) for a single ACE operating in a redundancy configuration. You must configure a maximum of two ACEs (peers) for redundancy to fail over from the active ACE to the standby ACE.

Note: All FT parameters are configured in the Admin context.
This configuration addresses the following redundancy components:

- A dedicated FT VLAN for communication between the members of an FT group. You must configure this same VLAN on both peers.
- An FT peer definition.
- An FT group that is associated with the Admin context.
- A critical tracking and failure detection process for an interface.

```
access-list ACL1 line 10 extended permit ip any any

class-map type management match-any L4_REMOTE-MGT_CLASS
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any
  5 match protocol http any
  7 match protocol snmp any
  8 match protocol https any

policy-map type management first-match L4_REMOTE-MGT_POLICY
  class L4_REMOTE-MGT_CLASS
    permit

interface vlan 100
  ip address 192.168.83.219 255.255.255.0
  peer ip address 192.168.83.230 255.255.255.0
  alias 192.168.83.200 255.255.255.0
  access-group input ACL1
  service-policy input L4_REMOTE-MGT_POLICY
  no shutdown

ft interface vlan 200
  ip address 192.168.1.1 255.255.255.0
  peer ip address 192.168.1.2 255.255.255.0
  no shutdown

ft peer 1
  ft-interface vlan 200
  heartbeat interval 300
  heartbeat count 10

ft group 1
  peer 1
  priority 200
  associate-context Admin
  inservice

ft track interface TRACK_VLAN100
  track-interface vlan 100
```

```
  peer track-interface vlan 200
  priority 50
  peer priority 5

ip route 0.0.0.0 0.0.0.0 192.168.83.1
```

Troubleshooting ACE Redundancy

This section describes the methods and CLI commands that you can use to troubleshoot redundancy issues in your ACE.

1. Ensure that the software versions and licenses installed in the two ACEs are identical. A software or license mismatch may generate the following syslog message:

```
%ACE-1-727006: HA: Peer is incompatible due to error str. Cannot be Redundant.
```

To verify the software (SRG) and license compatibility of the FT peer, enter the following command:

```
ACE_5/Admin# show ft peer status

Peer Id                     : 1
State                       : FSM_PEER_STATE_MY_IPADDR
Maintenance mode            : MAINT_MODE_OFF
SRG Compatibility           : COMPATIBLE
License Compatibility       : COMPATIBLE
FT Groups                   : 1
```

If the software or license is incompatible, install the appropriate software image or license in the peer to correct the problem.

2. Ensure that any SSL certificates (certs) and keys that exist in the active ACE are also configured in the standby ACE. SSL certs and keys are not synchronized automatically from the active to the standby. Use the **crypto export** and **crypto import** commands to accomplish this task. This requirement also applies to scripts and scripted probes. Failure to keep the active and standby configurations identical will cause configuration synchronization to fail and may cause the standby ACE to enter the STANDBY_COLD state.

3. The ACE sends heartbeat packets via UDP over the FT VLAN between peers. When heartbeats are not received during the specified interval (the interval and count are configurable), the ACE notifies the HA processor on the CP by sending a Peer_Down interprocess communication protocol (IPCP) message. If a peer is down or unreachable, you may receive one of the following syslog messages:

```
%ACE-1-727001: HA: Peer IP address is not reachable. Error: error str

%ACE-1-727002: HA: FT interface interface name to reach peer IP address is down. Error: error str
```

4. Verify connectivity between the peers over the FT VLAN. If a peer device is physically up but connectivity is the problem, you may end up with two active devices. If connectivity is lost due to the peer going down, reboot the peer to restore redundancy between the two devices.

5. Display heartbeat statistics, including missed heartbeats, by entering the following command:

```
ACE_5/Admin# show ft stats
HA Heartbeat Statistics
-----------------------

Number of Heartbeats Sent                : 0
Number of Heartbeats Received            : 0
```

```
Number of Heartbeats Missed               : 0
Number of Unidirectional HB's Received    : 0
Number of HB Timeout Mismatches           : 0
Num of Peer Up Events Sent                : 0
Num of Peer Down Events Sent              : 0
Successive HB's miss Intervals counter    : 0
Successive Uni HB's recv counter          : 0
```

6. Provide an alternate path for the ACE to check the peer's status in case of missed heartbeats and configure a query interface using the followng commands:

```
ACE_5/Admin# config
Enter configuration commands, one per line.  End with CNTL/Z.
ACE_5/Admin(config)# ft peer 1
ACE_5/Admin(config-ft-peer)# query-interface vlan 100
```

If the query interface is configured, upon receiving a PEER_DOWN message from the heartbeat process, the ACE data plane attempts to ping the peer using the Query VLAN. If the ping fails, the standby transitions to the ACTIVE state. If the ping is successful, the standby transitions to the STANDBY_COLD state. To recover from the STANDBY_COLD state, reboot the standby.

7. Each peer uses a VMAC that is dependent on the FT group number. If you are using multiple ACE modules in the same chassis, be careful when you configure the same FT groups in more than one module.

Display the VMAC for an FT group by entering the following command:

```
ACE_5/Admin# show interface internal iftable vlan100
vlan100
--------
ifid:           6
Context:        0
ifIndex:        16777316
physid:         100
rmode:          0 (unknown)
iftype:         0 (vlan)
bvi_bgid:       0
MTU:            1500
MAC:            00:18:b9:a6:91:15
VMAC:           00:00:00:00:00:00 <------- Virtual MAC Address
Flags:          0x8a000800 (valid, down, admin-down, Non-redundant, tracked)
ACL In:         0
ACL Out:        0
Route ID:       0
FTgroupID:      0
Zone ID:        6
Sec Level:      0
L2 ACL:         bpdu DENY, ipv6 DENY, mpls DENY, all DENY

LastChange:     0 (Thu Jan  1 00:00:00 1970)
iflookup index: 100
vlan-vmac index:0
Next Shared IF: 0
Lock:           Unlocked, seq 5
Lock errors:    0
Unlock errors:  0
No. of times locked:    5
No. of times unlocked:  5
Current/last owner:     0x40a7fc
```

8. If the members of an FT group are unable to reach the ACTIVE or the STANDBY_HOT state, there may be a context name mismatch for the same FT group. You may receive the following syslog message:

```
%ACE-1-727003: HA: Mismatch in context names detected for FT group FTgroupID. Cannot be redundant.
```

Be sure that the context names within the same FT group are identical on both ACEs.

9. Check the FT group configuration on both devices. Make sure that both devices are associated with the same context. Enter the following command:

```
ACE_5/Admin# show running-config ft
```

10. Verify the FT peer status and configuration by entering the following command:

```
ACE_5/Admin# show ft peer detail

Peer Id                       : 1
State                         : FSM_PEER_STATE_COMPATIBLE
Maintenance mode              : MAINT_MODE_OFF
FT Vlan                       : 100
FT Vlan IF State              : DOWN
My IP Addr                    : 10.1.1.1
Peer IP Addr                  : 10.1.1.2
Query Vlan                    : 110
Query Vlan IF State           : DOWN
Peer Query IP Addr            : 172.25.91.202
Heartbeat Interval            : 300
Heartbeat Count               : 20
Tx Packets                    : 318573
Tx Bytes                      : 66301061
Rx Packets                    : 318540
Rx Bytes                      : 66272840
Rx Error Bytes                : 0
Tx Keepalive Packets          : 318480
Rx Keepalive Packets          : 318480
TL_CLOSE count                : 0
FT_VLAN_DOWN count            : 0
PEER_DOWN count               : 0
SRG Compatibility             : COMPATIBLE
License Compatibility         : COMPATIBLE
FT Groups                     : 3
```

11. Verify the FT group status and configuration by entering the following command:

```
ACE_5/Admin# show ft group detail

FT Group                      : 1
No. of Contexts               : 1
Configured Status             : in-service
Maintenance mode              : MAINT_MODE_OFF
My State                      : FSM_FT_STATE_ACTIVE
My Config Priority            : 110
My Net Priority               : 110
My Preempt                    : Enabled
Peer State                    : FSM_FT_STATE_STANDBY
Peer Config Priority          : 100
Peer Net Priority             : 100
Peer Preempt                  : Enabled
Peer Id                       : 1
Last State Change time        : Thu Apr  2 00:00:00 2009
Running cfg sync enabled      : Enabled
```

```
Running cfg sync status      : Running configuration sync has completed
Startup cfg sync enabled     : Enabled
Startup cfg sync status      : Running configuration sync has completed
Bulk sync done for ARP: 0
Bulk sync done for LB: 0
Bulk sync done for ICM: 0
```

For information on troubleshooting the FT group status, see the "FT Group Status Conditions"

FT Peer and Group Status Details

This section describes how to diagnose unexpected status conditions for the FT group and FT peer. This information may enable you to troubleshoot an issue directly or help you to provide additional information to your Cisco support representative.

FT Group Status Conditions

This section describes how to diagnose and troubleshoot unexpected status conditions applicable to the FT group status.

STANDBY_COLD

An FT group status of STANDBY_COLD may appear when:

- Config sync fails (including, incr-sync and bulk-sync), or
- FT VLAN is down while the query interface is up

Config Sync Failure

In configuration synchronization fails, the peers are not correctly exchanging configuration information. This failure can be identified as follows:

1. Output of the **show ft peer detail** command shows that the peer state is "Compatible".
2. Entering **show ft group detail** shows that the FT group is in "Standby Cold" mode and entering **cfg sync status** shows the reason for the failure. For incr-sync failure, the output shows exactly which command resulted in an execution error on the standby. For a bulk-sync failure, the reason is "Error on Standby device when applying configuration file replicated from active".
3. To further investigate a bulk-sync failure, perform these steps on the standby device:
    - ◊ For software version A2(2.0) and earlier and version A2(1.3) and earlier releases, from the Admin context, enter **show ft history cfg_cntlr** and grep for "error:" to find any CLI commands that caused execution errors.
    - ◊ For later releases, enter **show ft config-error *ctx_name*** to view the failed CLI commands.

To work around a bulk sync failure, perform these steps to remove the CLI commands that triggered the error (as identified from the preceding analysis) and then retrigger the bulk sync operation, as follows:

1. Retrigger bulk sync by disabling config sync with the **no ft auto-sync running** command in configuration mode in the affected context.
2. Re-enable config sync with **ft auto-sync running**.

If the problem persists, repeat the above sequence until you eliminate the CLI command that triggered the problem.

FT VLAN Down with Query Interface Up

This condition can be identified by:

1. Entering **show ft peer detail**, which shows a peer state of FT_VLAN_DOWN.
2. Entering **show ft stats**, which shows that heartbeats are being missed.

In this case, check the physical connectivity of the device. It might be a physical port or cable issue.

STANDBY_CONFIG

If a device appears to be stuck in the STANDBY_CONFIG state:

1. Run **show ft history cfg_cntlr** to determine whether the peer devices successfully exchanged notifications regarding configuration synchronization.
2. Grep for the keywords MTS_OPC_REQ_CFG_DNLD_STATUS and MTS_OPC_CFG_DNLD_STATUS.

If one or both of the messages are missing, an error occurred in the synchronization exchange process.

Note that once it is stuck in the STANDBY_CONFIG state, configuration mode will be disabled on both the active and standby devices. It can be stuck in this state for up to 4 hours, after which a timeout period expires.

FT Peer Status Conditions

This section describes how to diagnose and troubleshoot unexpected status conditions applicable to the FT peer.

PEER_DOWN

If the peer status shows PEER_DOWN:

1. Check whether IP addresses for the local and peer device are configured correctly on both.
2. Verify that pinging or telneting to the peer IP address works. If ping fails, check whether the interface is up (**show interface**). If so, the interface VLAN is probably not allocated to the ACE module on the supervisor (which suggests a configuration issue on the supervisor).
3. Enter **show arp** to see if the FT peer IP address is resolved. (If ARP is not resolved and ping/telnet also failed, it might be an encapsulation issue requiring support).
4. Enter **show conn** on both sides to see if HA connections have been set up. If connections have not been set up, check the HA DP manager log (**show ft history ha_dp_mgr**). Setup may have failed for various reasons. If this is the case, contact Cisco technical support.
5. Enter **show ft stats** on both devices to see if heartbeats are being sent or received. If the Number of Heartbeats Missed counter is incrementing, the heartbeat packets could be getting dropped. Enter **show np 1 me-stats -sfp** to see if heartbeat packets are being received and forwarded to X-Scale, as indicated by the counter **Packets forward to XScale**. If this counter is not incrementing, provide the information to Cisco technical support.

TL_ERROR

This state may occur when the telnet connection used to exchange configuration information between the peers cannot be established but heartbeat packets are exchanged successfully. To identify this issue:

1. Verify that heartbeats are flowing by checking the statistics, **show ft stats**.
2. Attempt to connect by telnet or to ping the FT peer. The telnet connection attempt will likely fail.
3. Run **show arp** to see if the FT peer IP address can be resolved.

If **show arp** indicates that the address is not resolvable and the ping or telnet connect attempts fail, it is likely an encapsulation issue on the ACE.

FT_VLAN_DOWN

This state typically occurs when the FT VLAN goes down while the query interface is up. If the heartbeat exchange fails and the query interface is determined to be up based on an ICMP message check, the status is FT_VLAN_DOWN.

To verify, attempt to connect to the FT VLAN Peer IP address by ping or telnet.

If running **show ft stats** indicates that heartbeats are being missed, it is likely a physical connectivity issue, such as the physical port or cable failure.

FSM_PEER_STATE_ERROR

This indicates a Software Relationship Graph (SRG) version inconsistency between the peers. See the relationship graph table in the following section.

About WARM_COMPATIBLE and STANDBY_WARM

While peers in a redundant configuration are designed to operate with identical versions of the software, when you are upgrading or downgrading the software in the ACEs, it is possible for the peers to temporarily employ different software versions. The WARM_COMPATIBLE and STANDBY_WARM redundancy states help minimize the operational impact of CLI compatibility issues between the peers, and allow failovers to occur on a best-effort basis during such transitions.

When you upgrade or downgrade the ACE software in a redundant configuration with different software versions, the STANDBY_WARM and WARM_COMPATIBLE states allow the configuration and state synchronization process between the peers to continue on a best-effort basis. This basis allows the active ACE to synchronize configuration and state information with the standby even though the standby may not recognize or understand the CLI commands or state information.

In the STANDBY_WARM state, as with the STANDBY_HOT state, configuration mode is disabled on the standby ACE and configuration and state synchronization continues. A failover from the active to the standby based on priorities and preempt can still occur while the standby is in the STANDBY_WARM state. However, while stateful failover is possible for a WARM standby, it is not guaranteed. In general, modules should be allowed to remain in this state only for a short period of time.

When redundancy peers run different software versions, the SRG compatibility field shown by the **show ft peer status** command output displays WARM_COMPATIBLE instead of COMPATIBLE. When the peer is in the WARM_COMPATIBLE state, the FT groups in the standby transition to the STANDBY_WARM state instead of the STANDBY_HOT state.

The following software version combinations tables indicate whether the SRG compatibility field will display WARM_COMPATIBLE (WC) or COMPATIBLE (C):

ACE Module: C = COMPATIBLE / WC = WARM_COMPATIBLE

Active(Column)/Standby(Row)	A2(1.5)	A2(1.6)	A2(2.0)	A2(2.1)	A2(2.2)	A2(3.0)	A2(2.3)

A2(1.5)	C	WC	C	C	WC	WC	WC
A2(1.6)	WC	C	C	WC	WC	WC	WC
A2(2.0)	C	C	C	C	C	C	C
A2(2.1)	C	WC	C	C	WC	WC	WC
A2(2.2)	WC	WC	C	WC	C	WC	WC
A2(3.0)	WC	WC	C	WC	WC	C	WC
A2(2.3)	WC	WC	C	WC	WC	WC	C

ACE Appliance: C = COMPATIBLE / WC = WARM_COMPATIBLE

Active(Column)/Standby(Row)	A3(1.0)	A3(2.0)	A3(2.1)	A3(2.2)	A3(2.3)	A3(2.4)
A3(1.0)	C	C	C	C	WC	WC
A3(2.0)	C	C	C	C	WC	WC
A3(2.1)	C	C	C	C	WC	WC
A3(2.2)	C	C	C	C	WC	WC
A3(2.3)	WC	WC	WC	WC	C	WC
A3(2.4)	WC	WC	WC	WC	WC	C