This article introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when you configure and use 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 the ACE Troubleshooting Process

To troubleshoot your ACE, follow these general guidelines:

1. Maintain a consistent and recommended software version across all your ACEs. See the "Verifying the ACE Image" section.
2. See the ACE module release notes for your software version for the latest features, operating considerations, caveats, and CLI command changes.
3. Before you introduce configuration changes, use the ACE checkpoint feature to bookmark a known good configuration and save your configuration. If you run into problems with the new configuration, you can roll back the new configuration to the known good configuration. See the *Cisco Application Control Engine Module Administration Guide*. Troubleshoot new configuration changes immediately after adding them.
4. Verify that your configuration is correct for your network application. Make any required changes to the running-config file, and then test the configuration. If it is satisfactory, save it to the startup-config file using the **copy running-config startup-config** command for a particular virtual context or the **write memory** command from the Admin context to copy all running-config files in every virtual context to their respective startup-config files.
5. Enable system message logging. See the "Enabling ACE Logging" section.
6. Gather information that defines the specific symptoms. See the "Gathering ACE Troubleshooting Information" section.
7. Verify the physical connectivity between your device and end devices. See the "Verifying the Physical Connectivity Between the ACE and the End Hosts" section.
8. Verify the ACE Layer 2 connectivity. See the "Verifying the ACE Layer 2 Connectivity" section.
9. Verify the ACE end-to-end connectivity and the routing configuration. See the "Verifying the ACE Layer 3 Connectivity" section.
10. After you have determined that your troubleshooting attempts have not resolved the problem, contact the Cisco Technical Assistance Center (TAC) or your technical support representative. See the "Contacting Cisco Technical Support" section.

Verifying the ACE Image

To display the version of the software image and the image filename that is currently running in your ACE, enter the following command:

```
ACE_module5/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, 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.

Software
  loader:    Version 12.2[121]
  system:    Version A2(2.0) [build 3.0(0)A2(2.0)]  <--------
  system image file: [LCP] disk0:c6ace-t1k9-mzg.A2_2_0.bin  <--------
  installed license: no feature license is installed

Hardware
  Cisco ACE (slot: 5)
  cpu info:
    number of cpu(s): 2
    cpu type: SiByte
```

```
    cpu: 0, model: SiByte SB1 V0.2, speed: 700 MHz
    cpu: 1, model: SiByte SB1 V0.2, speed: 700 MHz
  memory info:
    total: 955396 kB, free: 289704 kB
    shared: 0 kB, buffers: 2336 kB, cached 0 kB
  cf info:
    filesystem: /dev/cf
    total: 1000000 kB, used: 494912 kB, available: 505088 kB

last boot reason:  NP 1 Failed : NP ME Hung

configuration register:  0x1
ACE_module5 kernel uptime is 4 days 22 hours 42 minute(s) 41 second(s)
```

This command provides other useful information, for example:

- Slot in which the ACE resides in the Catalyst 6500 series switch (in this case, slot 5)
- Available control plane memory
- Last boot reason
- Configuration register (confreg) value (0x0 boot to rommon, 0x1 boot using boot string)
- ACE uptime

Enabling ACE Logging

To enable logging on the ACE module and to send system logging (syslog) messages to the monitor, enter the following commands:

```
ACE_module5/Admin(config)# logging enable
ACE_module5/Admin(config)# logging monitor 7
ACE_module5/Admin(config)# exit
ACE_module5/Admin# terminal monitor
```

Note: Use the **terminal no monitor** command to stop viewing log messages in your remote session.

For more information about logging, see the "Troubleshooting with ACE Logging" section.

Gathering ACE Troubleshooting Information

The following sections recommend ways to gather information that is relevant to the problem that is occurring.

Rebooting the ACE

Do not reboot the ACE unless it is absolutely necessary. Some information that is important to troubleshooting your problem may not survive a reboot. Try to gather as much information as possible before rebooting.

Using show Commands

You can use a number of **show** commands in Exec mode to gather information specific to the symptoms you are observing in your ACE. In most cases, you can gather the information you need to troubleshoot the ACE by entering the **show tech-support** command. This command runs many **show** commands that are useful for troubleshooting the ACE. You can redirect the output of the **show tech-support** command to one the following destinations:

```
ACE_module5/Admin# show tech-support > ?
<File>     Name of file to redirect stdout.
disk0:     Enter the URI to redirect the output.
ftp:       Enter the URI to redirect the output.
sftp:      Enter the URI to redirect the output.
tftp:      Enter the URI to redirect the output.
volatile:  Enter the URI to redirect the output.
```

Capturing Packets in Real Time

Capturing packets (sometimes referred to as a "TCP dump") is a useful aid in troubleshooting connectivity problems with the ACE or for monitoring suspicious activity. The ACE can track packet information for network traffic that passes through the ACE. The attributes of the packet are defined by an ACL. The ACE buffers the captured packets, and you can copy the buffered contents to a file in Flash memory on the ACE or to a remote server. You can also display the captured packet information on your console or terminal.

The ACE captures packets subject to the following guidelines:

- One capture session is used per context
- Capture is triggered at flow setup
- Capture is configured on the client interface where the flow is received

Note: Probe traffic will not hit a security ACL, so ACLs cannot control the capture of those packets. Therefore, probe traffic cannot be captured by the packet capture utility.

If possible, you should capture packets using the ACE packet capturing utility before and after symptoms appear. Save the packet captures to a file.

To capture packets in real time, follow these steps:

1. Create an ACL for packet capturing or use an existing ACL if it meets the packet capture requirements by entering the following command:

```
ACE_module5/Admin(config)# access-list FILTER line 10 extended permit tcp any any eq www
ACE_module5/Admin# exit
```

2. Enter the **capture** command, for example:

```
ACE_module5/Admin# capture CAPTURE1 interface vlan 200 access-list FILTER
```

Note: Ensure that the ACL you specify in the **capture** command is for an input interface. If you configure the packet capture on the output interface, the ACE will fail to match any packets.

3. Display the capture status to determine the capture status and the buffer size by entering the following command:

```
ACE_module5/Admin# show capture CAPTURE1 status

Capture session : TEST
Buffer size     : 64 K
Circular        : no
Buffer usage    : 0.00%
Status          : stopped
```

Notice that the capture has not started yet. The default buffer size is 64 KB. You can specify a maximum of buffer size of 5000 KB and you can specify a circular buffer.

4. Start the packet capture on the ACE by entering the following command:

```
ACE_module5/Admin# capture CAPTURE1 start
11:56:15.354930 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 62: 209.165.201.10.4144 > 172.16.1.100.80: S [b
11:56:15.355257 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 62: 209.165.201.10.4144 > 192.168.1.11.80: S [
11:56:15.355669 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 58: 192.168.1.11.80 > 209.165.201.10.4144: S
11:56:15.355979 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 58: 172.16.1.100.80 > 209.165.201.10.4144: S [b
11:56:15.356442 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 56: 209.165.201.10.4144 > 172.16.1.100.80: . [t
11:56:15.356839 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 56: 209.165.201.10.4144 > 192.168.1.11.80: . [
11:56:15.357203 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 494: 209.165.201.10.4144 > 172.16.1.100.80: P [
11:56:15.357918 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 494: 209.165.201.10.4144 > 192.168.1.11.80: P
11:56:15.358436 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 56: 192.168.1.11.80 > 209.165.201.10.4144: .
11:56:15.358582 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 56: 172.16.1.100.80 > 209.165.201.10.4144: . [b
11:56:15.358822 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 272: 192.168.1.11.80 > 209.165.201.10.4144: P
11:56:15.359106 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 272: 172.16.1.100.80 > 209.165.201.10.4144: P [
11:56:15.359391 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 407: 192.168.1.11.80 > 209.165.201.10.4144: P
11:56:15.359751 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 407: 172.16.1.100.80 > 209.165.201.10.4144: P [
11:56:15.360101 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 56: 192.168.1.11.80 > 209.165.201.10.4144: F
11:56:15.360238 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 56: 172.16.1.100.80 > 209.165.201.10.4144: F [b
11:56:15.360378 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 56: 209.165.201.10.4144 > 172.16.1.100.80: . [t
11:56:15.360523 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 56: 209.165.201.10.4144 > 192.168.1.11.80: . [
11:56:15.360686 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 56: 209.165.201.10.4144 > 172.16.1.100.80: . [t
11:56:15.360831 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 56: 209.165.201.10.4144 > 192.168.1.11.80: . [
11:56:15.360973 0:1c:f9:9:18:0 0:b:fc:fe:1b:1 0800 56: 209.165.201.10.4144 > 172.16.1.100.80: F [t
11:56:15.361130 0:b:fc:fe:1b:1 0:c:29:f3:cd:e6 0800 56: 209.165.201.10.4144 > 192.168.1.11.80: F [
11:56:15.361290 0:c:29:f3:cd:e6 0:18:b9:a6:89:d 0800 56: 192.168.1.11.80 > 209.165.201.10.4144: .
11:56:15.361436 0:b:fc:fe:1b:1 0:1c:f9:9:18:0 0800 56: 172.16.1.100.80 > 209.165.201.10.4144: . [b
```

```
ACE_module5/Admin# capture CAPTURE1 stop
```

5. Copy the packet capture to disk0: by entering the following command:

```
ACE_module5/Admin# copy capture CAPTURE1 disk0:CAPTURE1
```

You can also copy the packet capture to an FTP, SFTP, or TFTP server.

6. Display the messages and connections within a packet capture by entering the following command:

```
ACE_module5/Admin# show capture CAPTURE1
0001: msg_type: ACE_HIT   ace_id: 637          action_flag: 0x3
0002: msg_type: CON_SETUP con_id: 1308623156    out_con_id: 167772463
0003: msg_type: PKT_RCV   con_id: 1308623156  other_con_id: 0
0004: msg_type: PKT_XMT   con_id: 167772463   other_con_id: 0
0005: msg_type: PKT_RCV   con_id: 167772463   other_con_id: 0
0006: msg_type: PKT_XMT   con_id: 1308623156  other_con_id: 0
<snip>
0025: msg_type: PKT_RCV   con_id: 167772463   other_con_id: 0
0026: msg_type: PKT_XMT   con_id: 1308623156  other_con_id: 0
0027: msg_type: CON_CLOSE con_id: 167772463         reason: 0
0028: msg_type: CON_CLOSE con_id: 1308623156        reason: 0
```

7. Display the details of each packet within a capture by entering the following command:

```
ACE_module5/Admin# show capture CAPTURE1 detail
0001: msg_type: ACE_HIT
ace_id: 637             action_flag: 0x3
src_addr: 209.165.201.10           src_port: 4144
dst_addr: 172.16.1.100     dst_port: 80
l3_protocol: 0          l4_protocol: 6
message_hex_dump:
```

```
0x0000: 0006 0104 0000 027d 0000 0000 d1a5 c90a  .......}........
0x0010: ac10 0164 0609 0013 1030 0050 0000 0000  ...d.....0.P....
0x0020: 0052 0000 05b4 0000 0000 027d 0300 0000  .R.........}....
0x0030: 0000 0040 0000 0000 0000 0000 0000 0000  ...@............
0x0040: 0000 0000 0000 0001                      ........

0002: msg_type: CON_SETUP
con_id: 1308623156       out_con_id: 167772463
src_addr: 209.165.201.10           src_port: 4144
dst_addr: 172.16.1.100     dst_port: 80
l3_protocol: 0          l4_protocol: 6
message_hex_dump:
0x0000: 0006 0101 4e00 0134 0a00 012f 0000 0000  ....N..4.../....
0x0010: d1a5 c90a ac10 0164 06e9 0013 1030 0050  .......d.....0.P
0x0020: e5b3 f25e 0012 0000 05b4 0100 0a00 012f  ...^...........
0x0030: 0000 0000 0018 0480 2445 0000 0000 0001  ........$E......
0x0040: 0000 0030 faf0 0010 05b4 0000 3008 e685  ...0........0...
0x0050: 0000 0000 e1ad 6b69 0000 0000 0000 027d  ......ki.......}
0x0060: 0000 0000 e1ad 6b69 0000 0000 0000 0000  ......ki........
0x0070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0080: c0a8 010b d1a5 c90a 06a1 0018 0050 1030  .............P.0
0x0090: 1a4c 0da2 0055 0000 05b4 0100 4e00 0134  .L...U......N..4
0x00a0: 0000 0000 0018 0480 2445 0022 0000 0000  ........$E."....
0x00b0: 0000 0000 0000 0000 05b4 0000 0000 0000  ................
0x00c0: 4a54 f427 e1ad 6b6b 0000 0000 0000 027d  JT.'..kk.......}
0x00d0: 0000 0000 e1ad 6b6b 0000 0000 0000 0000  ......kk........
0x00e0: 0000 0000 0000 0000 0000 0000            ............

0003: msg_type: PKT_RCV
con_id: 1308623156              other_con_id: 0
message_hex_dump:
0x0000: 0500 0050 0050 8034 0008 0014 0010 1488  ...P.P.4........
0x0010: 0020 000b fcfe 1b01 001c f909 1800 0800  ................
0x0020: 4500 0030 0933 4000 7f06 aa70 d1a5 c90a  E..0.3@....p....
0x0030: ac10 0164 1030 0050 3008 e684 e5b3 f25e  ...d.0.P0......^
0x0040: 7002 faf0 18fd 0000 0204 05b4 0101 0101  p...............

0004: msg_type: PKT_XMT
con_id: 167772463               other_con_id: 0
message_hex_dump:
0x0000: 4010 0050 0050 8034 0000 0028 0000 0088  @..P.P.4...(....
0x0010: 0004 000c 29f3 cde6 000b fcfe 1b01 0800  ....)...........
0x0020: 4500 0030 0933 4000 7f06 aa70 d1a5 c90a  E..0.3@....p....
0x0030: c0a8 010b 1030 0050 4a54 f426 0000 0000  .....0.PJT.&....
0x0040: 7002 faf0 18fd 0000 0204 05b4 0101 0101  p...............

0005: msg_type: PKT_RCV
con_id: 167772463               other_con_id: 0
message_hex_dump:
0x0000: 0500 004c 0050 8034 0008 0028 0010 2888  ...L.P.4...(..(.
0x0010: 0020 0018 b9a6 890d 000c 29f3 cde6 0800  ..........).....
0x0020: 4500 002c 0000 4000 4006 de68 c0a8 010b  E..,..@.@..h....
0x0030: d1a5 c90a 0050 1030 46ca 2127 4a54 f427  .....P.0F.!'JT.'
0x0040: 6012 16d0 6df5 0000 0204 05b4            `...m.......

0006: msg_type: PKT_XMT
con_id: 1308623156              other_con_id: 0
message_hex_dump:
0x0000: 4010 004c 0050 8034 0000 0014 0000 0088  @..L.P.4........
0x0010: 0004 001c f909 1800 000b fcfe 1b01 0800  ................
0x0020: 4500 002c 0000 4000 4006 de68 ac10 0164  E..,..@.@..h...d
0x0030: d1a5 c90a 0050 1030 2c7e 1385 3008 e685  .....P.0,~..0...
0x0040: 6012 16d0 6df5 0000 0204 05b4            `...m.......
```

```
0007: msg_type: PKT_RCV
con_id: 1308623156              other_con_id: 0
message_hex_dump:
0x0000: 0500 004a 0050 8034 0008 0014 0010 1488  ...J.P.4........
0x0010: 0020 000b fcfe 1b01 001c f909 1800 0800  ................
0x0020: 4500 0028 0934 4000 7f06 aa77 d1a5 c90a  E..(.4@....w....
0x0030: ac10 0164 1030 0050 3008 e685 2c7e 1386  ...d.0.P0...,~..
0x0040: 5010 faf0 05ad 0000 0000                 P.........

0008: msg_type: PKT_XMT
con_id: 167772463               other_con_id: 0
message_hex_dump:
0x0000: 4010 004a 0050 8034 0000 0028 0000 0088  @..J.P.4...(....
0x0010: 0004 000c 29f3 cde6 000b fcfe 1b01 0800  ....)...........
0x0020: 4500 0028 0934 4000 7f06 aa77 d1a5 c90a  E..(.4@....w....
0x0030: c0a8 010b 1030 0050 4a54 f427 46ca 2128  .....0.PJT.'F.!(
0x0040: 5010 faf0 05ad 0000 0000                 P.........

0009: msg_type: PKT_RCV
con_id: 1308623156              other_con_id: 0
message_hex_dump:
0x0000: 0500 0200 0050 8034 0008 0014 0010 1488  .....P.4........
0x0010: 0020 000b fcfe 1b01 001c f909 1800 0800  ................
0x0020: 4500 01e0 0935 4000 7f06 a8be d1a5 c90a  E....5@.........
0x0030: ac10 0164 1030 0050 3008 e685 2c7e 1386  ...d.0.P0...,~..
0x0040: 5018 faf0 a0bb 0000 4745 5420 2f73 6d61  P.......GET./sma
0x0050: 6c6c 2e68 746d 6c20 4854 5450 2f31 2e31  ll.html.HTTP/1.1
0x0060: 0d0a 486f 7374 3a20 3137 322e 3136 2e31  ..Host:.172.16.1
0x0070: 2e31 3030 0d0a 5573 6572 2d41 6765 6e74  .100..User-Agent

0010: msg_type: PKT_XMT
con_id: 167772463               other_con_id: 0
message_hex_dump:
0x0000: 4010 0200 0050 8034 0000 0028 0000 0088  @....P.4...(....
0x0010: 0004 000c 29f3 cde6 000b fcfe 1b01 0800  ....)...........
0x0020: 4500 01e0 0935 4000 7f06 a8be d1a5 c90a  E....5@.........
0x0030: c0a8 010b 1030 0050 4a54 f427 46ca 2128  .....0.PJT.'F.!(
0x0040: 5018 faf0 a0bb 0000 4745 5420 2f73 6d61  P.......GET./sma
0x0050: 6c6c 2e68 746d 6c20 4854 5450 2f31 2e31  ll.html.HTTP/1.1
0x0060: 0d0a 486f 7374 3a20 3137 322e 3136 2e31  ..Host:.172.16.1
0x0070: 2e31 3030 0d0a 5573 6572 2d41 6765 6e74  .100..User-Agent
<snip>
```

Note: If you view the ACE capture file in a third-party sniffer (for example, Wireshark), you will notice only the messages or type PKT_RCV and PKT_XMT are displayed. This situation is expected because the sniffer is not aware of the ACE's internal messaging.

Copying Core Dumps

If the ACE fails with a core dump, the core dump files may contain useful information. The core dump files reside in the core: directory. To view the contents of the core: directory, enter the following command:

```
ACE_module5/Admin# dir core:

  123589  Feb 22 00:34:20 2009 qnx_1_mecore_log.999.tar.gz
   30361  Feb 22 00:34:22 2009 ixp1_crash.txt

          Usage for core: filesystem
                    153950 bytes total used
                 202943138 bytes free
                 203097088 total bytes
```

You can copy the contents of the core: directory to several locations by using the **copy core:** command. The syntax of this command is as follows:

> **copy** {**core:***filename* | **disk0:**[*path*/]*filename* | **running-config** | **startup-config**} {**ftp://***server*/*path*[/*filename*] | **sftp://**[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*]}

The ACE provides core dumps for both the control plane and the data plane. Each core dump file contains the following information:

- Version
- Time of failure
- Number of CPUs
- Current CPU
- BKL status
- IRQ lock status
- Buffers

After Gathering Troubleshooting Information

After you have gathered all the above information, be prepared to send the information to your customer service representative or TAC. You can send the information in the following ways:

- FTP
- SFTP
- TFTP

Verifying the Physical Connectivity Between the ACE and the End Hosts

To verify the physical connectivity of the ACE, follow these steps:

1. Check all cable connections on the Catalyst 6500 series switch or Cisco 7600 series router that may impact the ACE.
2. Use the extended **ping** command to send an ICMP Echo request to the end devices.

```
ACE_module5/Admin# ping
Target IP address: 10.1.1.2
Repeat count [5]: 4
Datagram size [100]: 200
Timeout in seconds [2]: 10
Extended commands [n]: 4
Pinging 10.1.1.2 with timeout = 10, count = 4, size = 200 ....

Response from 10.1.1.2 :  seq 1 time 0.494 ms
Response from 10.1.1.2 :  seq 2 time 0.367 ms
Response from 10.1.1.2 :  seq 3 time 0.264 ms
Response from 10.1.1.2 :  seq 4 time 0.237 ms
4 packet sent, 4 responses received, 0% packet loss
```

If a host is one hop away and you are unable to reach the host, then ping the intermediary gateway. If the gateway is not reachable, enter the **show ip route** command and check to make sure that the correct route is displayed. For example, enter:

```
ACE_module5/Admin# show ip route

Routing Table for Context Admin (RouteId 0)

   Codes: H - host,   I - interface
          S - static,      N - nat
          A - need arp resolve,      E - ecmp

Destination         Gateway          Interface         Flags
--------------------------------------------------------------------
0.0.0.0             10.2.2.1      vlan130           S [0xc]
10.2.2.0/24      0.0.0.0          vlan130           IA [0x30]
172.27.15.0/24      0.0.0.0          vlan100           IA [0x30]
172.27.16.0/24      0.0.0.0          vlan200           IA [0x30]
172.19.110.0/26     0.0.0.0          vlan55            IA [0x30]
172.27.16.16/29     0.0.0.0          vlan200           N [0x280]
172.27.16.33/32     0.0.0.0          vlan100           N [0x280]

Total route entries = 7
```

If necessary, enter a static route for the gateway.

Verifying the ACE Layer 2 Connectivity

To verify the Layer 2 connectivity of the ACE, follow these steps:

1. Verify that the ARP table is populated with the IP addresses and corresponding MAC addresses of the ACE, the gateway, the local interface, and other IPs that the ACE has learned.

```
switch/Admin# show arp

Context Admin
================================================================================
IP ADDRESS      MAC-ADDRESS        Interface  Type      Encap  NextArp(s) Status
================================================================================
10.86.215.208   00.02.7e.39.51.9c  vlan130   LEARNED    5      2350 sec     up
10.86.215.228   00.e0.81.22.78.ff  vlan130   LEARNED    6      6379 sec     up
10.86.215.234   00.1a.a1.48.f3.44  vlan130   LEARNED    4      1114 sec     up
10.86.215.1     00.00.0c.07.ac.00  vlan130   GATEWAY    2      153 sec      up
10.86.215.2     00.11.5d.e1.2f.fc  vlan130   LEARNED    3      12054 sec    up
10.86.215.134   00.18.b9.a6.91.15  vlan130   INTERFACE  LOCAL     _         up
================================================================================
Total arp entries 6
```

2. Verify that the ACE is connected to the switch fabric of the Catalyst 6500 series switch or the Cisco 7600 series router. The ACE uses a 10-Gigabit Ethernet switch fabric interface (SFI) to connect to the chassis backplane as opposed to the CSM, which uses a port channel. The ACE uses the following format for this interface:

Te<slot>/1

For example, if the ACE is in slot 5, you can see the status of the backplane connection by entering the following command on the Catalyst 6500 series switch or the Cisco 7600 series router:

```
cat6k# show interface te5/1 status

Port    Name               Status       Vlan       Duplex  Speed Type
Te5/1                      connected    trunk         full    10G MultiService Module
```

If there is no output from this command, then either the ACE is not installed properly or the ACE is powered down.

3. Verify the association of the ACE MAC entries with the allocated VLAN interfaces. Enter the following command at the Supervisor CLI:

```
cat6k# show mac-address-table dynamic
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
.
.
.
*  130  0018.b9a6.9115   dynamic  Yes         40   Te5/1 <------- MAC address should be in the ran
.
.
.

cat6k# show module 5
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  5    1  Application Control Engine Module      ACE10-6500-K9      SAD1031044S

Mod MAC addresses                          Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  5  0018.b9a6.9114 to 0018.b9a6.911b   1.1   8.7(0.22)ACE A2(2.0)      Ok <------- MAC address ra

Mod  Online Diag Status
---- -------------------
  5  Pass
```

4. Check the status of the Te5/1 port to ensure that it is in the forwarding state by entering the following command:

```
cat6k# show spanning-tree vlan 130

MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     0001.632f.2c17
             Cost        200019
             Port        642 (GigabitEthernet6/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0011.bc06.f800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi2/14           Desg FWD 20000     128.142  P2p
Gi2/37           Desg FWD 200000    128.165  P2p
Te3/1            Desg FWD 2000      128.257  Edge P2p
Te5/1            Desg FWD 2000      128.513  Edge P2p
Gi6/2            Root FWD 200000    128.642  Shr Bound(STP)
Te8/1            Desg FWD 2000      128.897  Edge P2p
```

Verifying the ACE Layer 3 Connectivity

Use the **traceroute** command to check the route between the ACE and the end devices.

```
ACE_module5/Admin# traceroute 10.20.12.153
traceroute to 10.20.12.153 (10.20.12.153), 30 hops max, 40 byte packets
 1  10.20.215.2 (10.20.215.2)  0.532 ms  0.436 ms  0.362 ms
 2  10.20.239.161 (10.20.239.161)  0.421 ms  0.488 ms  0.404 ms
 3  10.20.238.93 (10.20.238.93)  0.471 ms  0.422 ms  0.413 ms
 4  172.27.16.177 (172.27.16.177)  0.488 ms  0.435 ms  0.430 ms
 5  172.27.16.226 (172.27.16.226)  0.474 ms  0.363 ms  0.368 ms
 6  192.168.0.134 (192.168.0.134)  0.624 ms  0.510 ms  0.494 ms
 7  10.20.12.153 (10.20.12.153)  23.982 ms  24.702 ms  25.976 ms
```

Contacting Cisco Technical Support

If you are unable to resolve a problem after using the troubleshooting suggestions in the articles in this wiki, contact the Cisco Technical Assistance Center (TAC) for assistance and further instructions. Before you call, have the following information ready to help your TAC engineer assist you as quickly as possible:

- Date that you received the ACE
- Chassis serial number (located on a label on the right side of the rear panel of the chassis)
- Type of software and release number (if possible, enter the **show version** command)
- Maintenance agreement or warranty information
- Brief description of the problem
- Brief explanation of the steps that you have already taken to isolate and resolve the problem

For information on steps to take before calling Technical Support, see the "Gathering ACE Troubleshooting Information" section.

You can reach TAC in several ways as follows:

- Create a service request online
- Call the TAC at the telephone numbers on this page.
- Contact the Cisco Small Business Support Center