This article describes how to troubleshoot issues involving ACE remote access.


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


# Contents


- 1 Overview of ACE Remote Access
- 2 Configuring a Management Policy for Remote Access
- 3 Troubleshooting Remote Access
  - 3.1 Troubleshooting Telnet
  - 3.2 Troubleshooting SSH
  - 3.3 Troubleshooting KAL-AP

## Overview of ACE Remote Access

You can access the ACE remotely using several different protocols as follows:

- HTTP
- HTTPS
- ICMP
- KALAP-UDP
- SSH
- SNMP
- Telnet

These protocols require that you configure a management traffic policy on the ACE and associate that policy with the interface that you intend to use for management traffic. A management policy allows the classification and distribution engine (CDE) to classify (match) incoming management traffic to the management policy and to forward that traffic to the control plane (CP). For complete details about remote access, see the *Cisco Application Control Engine Module Administration Guide (Software Version A2(1.0))*.

## Configuring a Management Policy for Remote Access

To configure a management policy that allows remote access to the ACE using ICMP, SSH, or Telnet, enter the following commands:

```
ACE_module5/Admin(config)# access-list ACL1 extended permit ip any any
ACE_module5/Admin(config)# class-map type management match-any MGMT_CLASS
ACE_module5/Admin(config-cmap-mgmt)# 2 match protocol icmp any
ACE_module5/Admin(config-cmap-mgmt)# 3 match protocol ssh any
ACE_module5/Admin(config-cmap-mgmt)# 4 match protocol telnet any
ACE_module5/Admin(config-cmap-mgmt)# exit
ACE_module5/Admin(config)# policy-map type management first-match MGMT_POLICY
ACE_module5/Admin(config-pmap-mgmt)# class MGMT_CLASS
ACE_module5/Admin(config-pmap-mgmt-c)# permit
ACE_module5/Admin(config-pmap-mgmt-c)# exit
ACE_module5/Admin(config-pmap-mgmt)# exit
ACE_module5/Admin(config)# interface vlan 100
ACE_module5/Admin(config-if)# ip address 192.168.12.15 255.255.255.0
ACE_module5/Admin(config-if)# service-policy input MGMT_POLICY
ACE_module5/Admin(config-if)# access-group input ACL1
```

## Troubleshooting Remote Access

If you cannot access the ACE module remotely, follow these steps:

1. Beginning with ACE software release A2(1.1), by default, the ACE CLI is only locally accessible either using the ACE console port or through the supervisor by entering the **session** command. Remote access to the ACE (for example, Telnet, SSH, and so on) is disabled until you change the admin user account password from the default. Access to the XML API is also disabled until you change the www user account password from the default. The ACE will display these warnings each time you access the CLI using the the console port or the supervisor until you change these passwords.

```
cat6k#session slot 5 processor 0
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
```

```
Trying 127.0.0.20 ... Open

ACE_module5 login: admin
Password:
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, 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.
Please change the password for admin user.
Admin user is allowed to login only from supervisor until the password is changed.
User 'www' is disabled. Please change the password to enable the user.
```

Use the following commands to change the passwords of the admin and www user accounts:

```
ACE_module5/Admin# config
Enter configuration commands, one per line.  End with CNTL/Z.
ACE_module5/Admin(config)# username admin password 0 cisco123 role Admin domain default-domain
ACE_module5/Admin(config)# username www password 0 cisco123 role Admin domain default-domain
ACE_module5/Admin(config)# exit
```

Note that, although the passwords were entered in clear text above, they will be stored in the ACE configuration in an encrypted format:

```
ACE_module5/Admin# show run | i username
Generating configuration....
username admin password 5 $1$M7gtcvBC$9ca78Q.ZH5jZpqDVuLnkN0  role Admin domain default-domain
username www password 5 $1$ulc7KHL5$2HlgNTEez03.ElmbiWKyY/  role Admin domain default-domain
```

2. Ensure that the remote access method protocol (for example, Telnet or SSH) that you are trying to use is configured in the management class map and that the management class has been permitted in the management policy. If necessary, correct your ACE configuration. To display your management policy configuration elements, enter the following Exec mode commands:

```
ACE_module5/Admin# show running-config class-map
Generating configuration....

class-map type management match-any MGMT_CLASS
  2 match protocol icmp any
  3 match protocol ssh any
  4 match protocol telnet any

ACE_module5/Admin# show running-config policy-map MGMT_POLICY
Generating configuration....

policy-map type management first-match MGMT_POLICY
  class MGMT_CLASS
    permit
  class class-default
```

3. Ensure that the management policy is applied to the correct interface and that you are using the correct IP address for that interface. If necessary, correct your configuration. Enter the following command:

```
ACE_module5/Admin# show running-config interface

interface vlan 100
  ip address 192.168.12.15 255.255.255.0
```

```
  access-group input ACL1
  access-group output ACL1
  service-policy input MGMT_POLICY
  no shutdown
```

4. Check the status of the management interface by entering the following command:

```
ACE_module5/Admin# show interface vlan 100

vlan100 is up
  Hardware type is VLAN
  MAC address is 00:18:b9:a6:91:15
  Mode : routed
  IP address is 192.168.12.15 netmask is 255.255.255.0
  FT status is non-redundant
  Description:not set
  MTU: 1500 bytes
  Last cleared: never
  Alias IP address not set
  Peer IP address not set
  Assigned from the Supervisor, up on Supervisor
     115303 unicast packets input, 74570169 bytes
     273637 multicast, 521226 broadcast
     0 input errors, 0 unknown, 0 ignored, 0 unicast RPF drops
     12591 unicast packets output, 2120271 bytes
     0 multicast, 4604 broadcast
     0 output errors, 0 ignored
```

5. If the interface is down, ensure that the **no shutdown** command is configured on the interface to enable it. If necessary, correct your configuration. Enter the following command:

```
ACE_module5/Admin# show running-config interface
```

6. Ensure that you have not exceeded the allocated resources for management connections or maximum management bandwidth by entering the following commands:

```
ACE_module5/Admin# show resource usage resource mgmt-connections
                                                    Allocation
        Resource         Current       Peak        Min        Max       Denied
-------------------------------------------------------------------------------
Context: Admin
  mgmt-connections              2         10          0     100000          0
Context: C1
  mgmt-connections              0          0          0     100000          0

ACE_module5/Admin# show resource usage resource rate mgmt-traffic
                                                    Allocation
        Resource         Current       Peak        Min        Max       Denied
-------------------------------------------------------------------------------
Context: Admin
    mgmt-traffic rate          78       3588          0  125000000          0
Context: C1
    mgmt-traffic rate           0          0          0  125000000          0
```

7. If necessary, allocate more resources to management connections by entering the following command:

```
ACE_module5/Admin(config-resource)# limit-resource mgmt-connections minimum number maximum number
```

8. Ensure that traffic is reaching the CP by entering the following command:

```
ACE_module5/Admin# show netio stats

High Priority (Control)              Normal Priority (Data)
-----------------------              ----------------------
Net Rx Packets        : 680          Net Rx Packets        : 10799640 <-------
Net Rx Bytes          : 52902        Net Rx Bytes          : 842376636 <-------
Net Rx Unsupported L2 : 0            Net Rx Unsupported L2 : 0
Net Rx Lock Errors    : 0            Net Rx Lock Errors    : 0
Net Rx Interface Miss : 0            Net Rx Interface Miss : 10470926
Net Rx No Arp Client  : 0            Net Rx No Arp Client  : 0
Net Rx Alias Drops    : 0            Net Rx Alias Drops    : 0
Net Rx Repl. Errors   : 0            Net Rx Repl. Errors   : 0
Net Rx Repl. If Err   : 0            Net Rx Repl. If Errs  : 0
Net Rx Internal Errs  : 0            Net Rx Internal Errs  : 0

Net Tx Packets        : 0            Net Tx Packets        : 10469 <-------
Net Tx Bytes          : 0            Net Tx Bytes          : 1194879 <-------
Net Tx Lock Errors    : 0            Net Tx Lock Errors    : 0
Net Tx Bad Context ID : 0            Net Tx Bad Context ID : 0
Net Tx No Route Found : 0            Net Tx No Route Found : 0
Net Tx No Adjacency   : 0            Net Tx No Adjacency   : 0
Net Tx Invalid If ID  : 0            Net Tx Invalid If ID  : 0
Net Tx If Down        : 0            Net Tx If Down        : 0
Net Tx No Src Addr    : 0            Net Tx No Src Addr    : 0
Net Tx No Encap       : 0            Net Tx No Encap       : 0
Net Tx FIFO Errors    : 0            Net Tx Fifo Errors    : 0
Net Tx No VMAC Errors : 0            Net Tx No VMAC Errors : 0

IPC Tx Packets        : 78           IPC Tx Packets        : 0
IPC Tx Bytes          : 17766        IPC Tx Bytes          : 0
IPC Tx Fifo Errors    : 0            IPC Tx Fifo Errors    : 0

Client Rx Queue Full  : 0            Client Rx Queue Full  : 0

Pseudo Rx Queue Full  : 0            Pseudo Rx Queue Full  : 0
```

Management traffic is considered to-the-ACE traffic or CP traffic. If traffic is reaching the CP, the Normal Priority (Data) Net Rx Packets, Net Rx Bytes, Net TX packets, and Net TX bytes counters should be increasing. If not, contact TAC.

9. If traffic is not arriving at the CP, ensure that traffic is reaching the classification and distribution engine (CDE) from the SFI by entering the following command:

```
ACE_module5/Admin# show cde health

CDE BRCM INTERFACE
======================
Packets received                                          10580
Packets transmitted                                    10802845
Broadcom interface CRC error count                            0
BRCM VOQ status                          [empty]      [not full]
BRCM pull status                                       [pulling]

CDE HYPERION INTERFACE
======================
Packets received                                       12312951 <-------
Packets transmitted                                       17361 <-------
Short packets drop count                                      0
Fifo Full drop count                                          0
Protocol error drop count                                     0
FCS error drop count                                          0
CRC error drop count                                          0
```

```
Num times flow control triggered on hyp interface                0
Num self generated multicast packets filtered               4618
HYP IXP0 VOQ status                       [empty]      [not full]
HYP IXP1 VOQ status                       [empty]      [not full]
HYP SLOW VOQ status                       [empty]      [not full]
HYP tx pull status                                      [pulling]

<snip>
```

If traffic is reaching the CDE, the Packets received and the CDE Hyperion Interface Packets transmitted counters should be increasing. If not, contact TAC.

10. If packets are not reaching the CDE, ensure that the MSFC in the Catalyst 6500 series switch or the Cisco 7600 series router is sending packets to the switch fabric interface (SFI) by entering the following command on the supervisor engine:

```
cat6k# show svclc module 5 traffic
ACE module 5:

Specified interface is up line protocol is up (connected)
  Hardware is C6k 10000Mb 802.3, address is 0018.b9a6.9114 (bia 0018.b9a6.9114)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is unsupported
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 1w2d
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     912150 packets input, 74727962 bytes, 0 no buffer
     Received 796374 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     17390 packets output, 2145844 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

If the MSFC is sending traffic to the SFI, the packets input and the packets output counters should be increasing. If not, contact TAC.

## Troubleshooting Telnet

If you cannot Telnet to the ACE, ensure that you have not reached the maximum connection limit for Telnet by entering the following commands:

```
ACE_module5/Admin# show telnet

Session ID     Remote Host         Active Time
4254           127.0.0.51  :41985    0: 8:13
```

The **show telnet** command output shows only one Telnet session. A maximum of 15 more users can potentially Telnet to the Admin context.

To display the maximum number of users allowed to Telnet to a particular context, enter the following command:

```
ACE_module5/Admin# show telnet maxsessions

Maximum Sessions Allowed is 16
```

## Troubleshooting SSH

If you attempt to connect to the ACE using SSH and receive the following error, follow these steps:

```
[linux]$ ssh admin@192.168.0.210
ssh_exchange_identification: Connection closed by remote host [linux]$
```

1. Ensure that SSH is enabled in the management policy by entering the following command:

```
ACE_module5/Admin# show running-config class-map

class-map type management match-any MGMT_CLASS
  2 match protocol http any
  3 match protocol https any
  4 match protocol icmp any
  6 match protocol ssh any <------- SSH is enabled
  7 match protocol telnet any
  8 match protocol snmp any

switch/Admin# show running-config policy-map MGMT_POLICY
Generating configuration....

policy-map type management first-match MGMT_POLICY
  class MGMT_CLASS
    permit <------- All protocols in the MGMT_CLASS class-map are permitted including SSH
```

2. Ensure that the SSH key has been generated by entering the following command:

```
switch/Admin# show ssh key
**************************************
could not retrieve rsa1 key information
**************************************
could not retrieve rsa key information
**************************************
could not retrieve dsa key information
**************************************
no ssh keys present. you will have to generate them
**************************************
```

The **show ssh key** command output shows that no SSH key has been generated.

3. Generate an SSH key based upon your security requirements by entering the following commands:

```
ACE_module5/Admin# config
Enter configuration commands, one per line.  End with CNTL/Z.
ACE_module5/Admin(config)# ssh key rsa 4096
generating rsa key(4096 bits).....
.......................
generated rsa key
ACE_module5/Admin(config)# exit
switch/Admin# show ssh key
dsa   rsa   rsa1
ACE_module5/Admin# show ssh key
```

```
**************************************
could not retrieve rsa1 key information
**************************************
rsa Keys generated:Tue Apr  7 15:55:20 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAgEAr3z0MO0knoS6YwntSxUkWDWjHZfFE7Y6nLd8qQVcPMu0
XpvkabDswLwoEdC9nOWM4v4g4PDpUz+tk+2WHJ4MMgRVeomVbK/2+Zx0Eds1p2XlhiV9KPcV
pflpNNt63Mr01oLHoHpjxJ8ubfJJ+gPhMoBmQyGKedQOk5tVlbOpyxS2f7yWGqzF26AzXTFFdS0xYEcN4GrtziduBlh4TYRxk9
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+9C0i
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+uowK
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+gHaa
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+ryoo
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+iKsh
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+/cut
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+7OvN
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+w6ig
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+msEF
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+XvRo
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+w34s
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+mbRk
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+e9p2
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+PEAQ
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+D+Ty
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+GsLz
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+EaKa
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+MNQm
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+VVkV
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+4d21
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+x6VH
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+fEGT
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+64zM
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+Hf/a
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+e9Tu
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+W4nD
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+7SUP
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+leL+
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+Tmwt
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+8ymk
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+20L0
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+ym2A
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+mfe5
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+A+Py
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+k/Dx
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+NeCF
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+mSK1
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+V747
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+M0xG
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+QiEP
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+CCTj
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+8lkb
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+GXOo
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+C094
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+eDPM
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+F+xp
ZAWROUVbRMFz1MjblIVX+C9nygSGeaMJ9KDosbUlQCBnOtWViPblov0lViwk4QEHAAL+eNj
zsFzc1023QU8xwlrhgvL0xXKxUmITV4y2VaSmEc/0RH/c4XAinNy955X6w9ejqXG9aYFjljLBtCHKXgyAZbQ48E4UPtPwPTCC3
/6x/6XVFPBw4okLcz6tVDLqn7dGiTEjzYgfQBwKXiIPrGg9EmBgwmQKWuJpOde+jbMD9kU1WmUoUWvTvPtXQ0=

bitcount:4096
fingerprint:
13:96:fe:f0:f7:d7:5f:9c:d7:2a:da:72:8a:93:53:a6
**************************************
could not retrieve dsa key information
```

```
*************************************

Now SSH should work.
```

4. Try connecting to the ACE via SSH again by entering the following command:

```
[linux]$ ssh admin@192.168.0.210
Warning: Permanently added '192.168.0.210' (RSA) to the list of known hosts.

Password:
Cisco Application Control Software (ACSW) TAC support: http://www.cisco.com/tac Copyright (c) 1985
The copyrights to certain works contained herein are owned by other third parties and are used and
Some parts of this software are covered under the GNU Public License. A copy of the license is ava
ACE_module5/Admin#
```

5. Confirm the SSH session from the ACE CLI by entering the following command:

```
ACE_module5/Admin# show ssh session-info

Session ID     Remote Host         Active Time
6986           10.76.248.6 :42116    0: 0:46
```

## Troubleshooting KAL-AP

To troubleshoot KAL-AP related issues, follow these steps:

1. Make sure that KAL-AP is enabled under the management policy by entering the following commands:

```
ACE_module5/Admin# show running-config class-map
Generating configuration....

class-map type management match-any MGMT_CLASS
  2 match protocol http any
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol kalap-udp any  <------- KAL-AP is enabled
  6 match protocol ssh any
  7 match protocol telnet any
  8 match protocol snmp any

ACE_module5/Admin# show running-config policy-map MGMT_POLICY
Generating configuration....

policy-map type management first-match MGMT_POLICY
  class MGMT_CLASS
    permit <------- All protocols in the MGMT_CLASS class-map are permitted including SSH
```

2. Verify that traffic from the Cisco Global Site Selector (GSS) is reaching the ACE module. KAL-AP statistics should get incremented.

```
ACE_module5/Admin# sh stats kalap

+-----------------------------------------------------+
+---------------- KAL-AP(UDP) statistics -------------+
+-----------------------------------------------------+

Total bytes received                : 243956
Total bytes sent                    : 184884
Total requests received             : 5100
Total responses sent                : 5100
```

```
Total requests successfully received : 5100
Total responses successfully sent    : 5100
Total secure requests received       : 0
Total secure responses sent          : 0
Total requests with errors           : 0
Total requests with parse errors     : 0
Total response transfer errors       : 0
-----------------------------------------------------
```

3. Allow secure KAL-AP requests, and add the GSS IP address and the shared secret to the ACE by entering the following commands:

```
ACE_module5/Admin# config
ACE_module5/Admin(config)# kalap udp
ACE_module5/Admin(config-kalap-udp)# ip address 192.168.10.52 encryption md5 cisco
                                                  (GSS IP)
```

4. Display information about the load VIP by entering the following command:

```
ACE_module5/Admin# show kalap udp load vip 10.1.1.1

Error: Vip object not found!
ACE_module5/Admin#
```

If the VIP object is not found while displaying the load value as shown above, check whether the VIP got downloaded in the configuration manager internal table by entering the following command:

```
ACE_module5/Admin# show cfgmgr internal table vip

VIP-Id      VIP-Addr                            Ctx-Id  Flags
---------------------------------------------------------------------------
1           10.1.1.1                             1      DATA_VALID,
L3Rule_list :-->: 41: 42
Load Value: 255  Load Time stamp: Wed Apr  8 05:10:20 2009
```