CHAPTER 77

Troubleshooting

This chapter describes how to troubleshoot the ASA, and includes the following sections:

Testing Your Configuration

This section describes how to test connectivity for the single mode ASA or for each security context, how to ping the ASA interfaces, and how to allow hosts on one interface to ping through to hosts on another interface.

We recommend that you only enable pinging and debugging messages during troubleshooting. When you are done testing the ASA, follow the steps in the "Disabling the Test Configuration" section on page 77-5.

This section includes the following topics:

Enabling ICMP Debugging Messages and Syslog Messages

Debugging messages and syslog messages can help you troubleshoot why your pings are not successful. The ASA only shows ICMP debugging messages for pings to the ASA interfaces, and not for pings through the ASA to other hosts. To enable debugging and syslog messages, perform the following steps:

	Command	Purpose
Step 1	`debug icmp trace`	Shows ICMP packet information for pings to the ASA interfaces.
Step 2	`logging monitor debug`	Sets syslog messages to be sent to Telnet or SSH sessions. **Note** You can alternately use the **logging buffer debug** command to send log messages to a buffer, and then view them later using the **show logging** command.
Step 3	`terminal monitor`	Sends the syslog messages to a Telnet or SSH session.
Step 4	`logging on`	Enables syslog message generation.

Examples

The following example shows a successful ping from an external host (209.165.201.2) to the ASA outside interface (209.165.201.1):

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

The output shows the ICMP packet length (32 bytes), the ICMP packet identifier (1), and the ICMP sequence number (the ICMP sequence number starts at 0, and is incremented each time that a request is sent).

Pinging ASA Interfaces

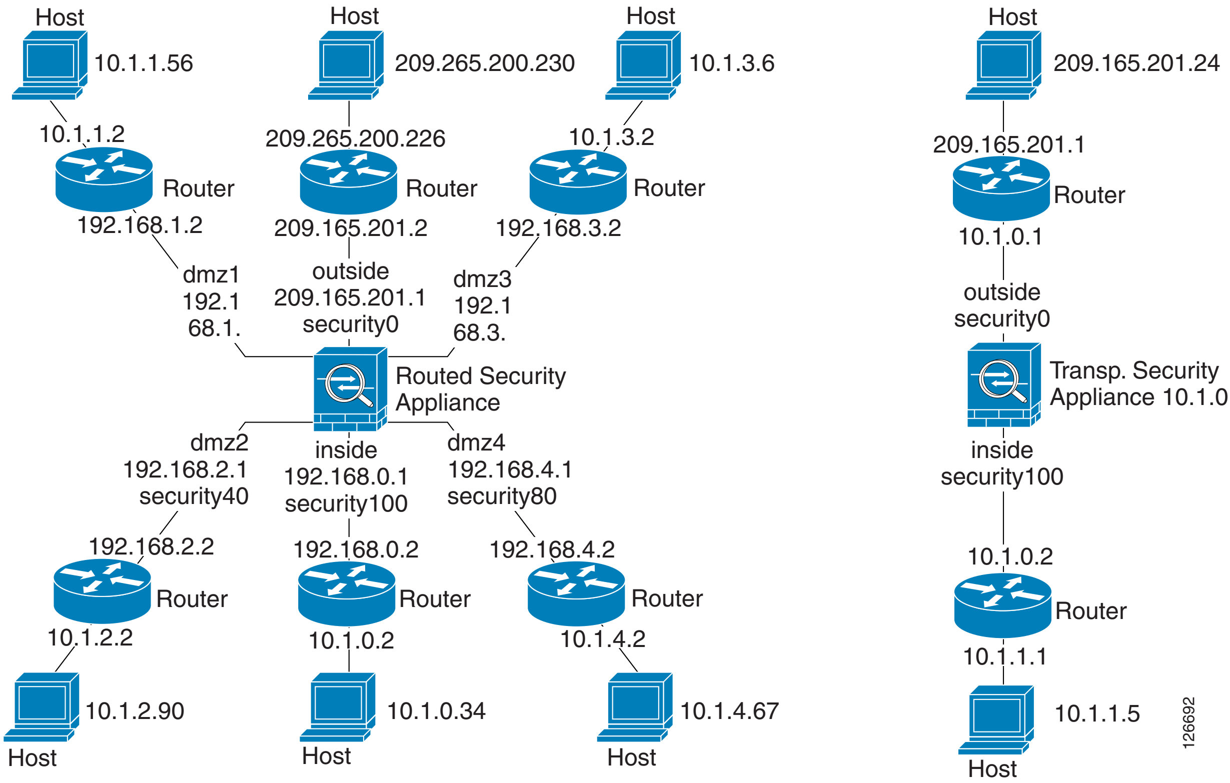
To test whether the ASA interfaces are up and running and that the ASA and connected routers are operating correctly, you can ping the ASA interfaces. To ping the ASA interfaces, perform the following steps:

Step 1 Draw a diagram of your single-mode ASA or security context that shows the interface names, security levels, and IP addresses.

Note Although this procedure uses IP addresses, the **ping** command also supports DNS names and names that are assigned to a local IP address with the **name** command.

The diagram should also include any directly connected routers, and a host on the other side of the router from which you will ping the ASA. You will use this information in this procedure and in the procedure in the "Passing Traffic Through the ASA" section on page 77-4. For example:

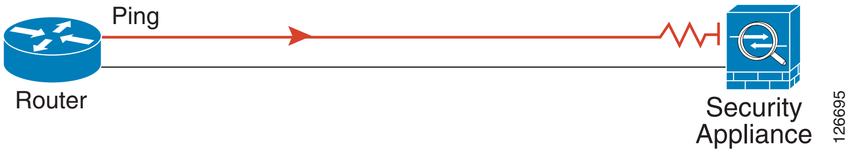
Figure 77-1 Network Diagram with Interfaces, Routers, and Hosts



Step 2 Ping each ASA interface from the directly connected routers. For transparent mode, ping the management IP address. This test ensures that the ASA interfaces are active and that the interface configuration is correct.

A ping might fail if the ASA interface is not active, the interface configuration is incorrect, or if a switch between the ASA and a router is down (see Figure 77-2). In this case, no debug messages or syslog messages appear, because the packet never reaches the ASA.

Figure 77-2 Ping Failure at the ASA Interface

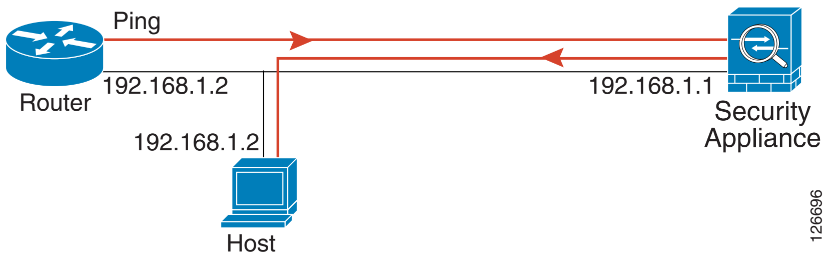


If the ping reaches the ASA, and it responds, debugging messages similar to the following appear:

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

If the ping reply does not return to the router, then a switch loop or redundant IP addresses may exist (see Figure 77-3).

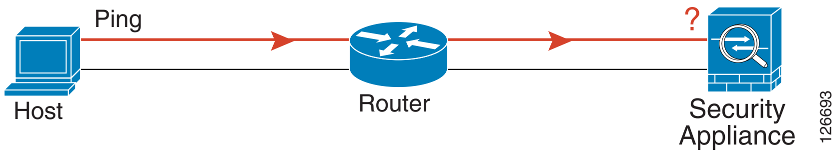
Figure 77-3 Ping Failure Because of IP Addressing Problems



Step 3 Ping each ASA interface from a remote host. For transparent mode, ping the management IP address. This test checks whether the directly connected router can route the packet between the host and the ASA, and whether the ASA can correctly route the packet back to the host.

A ping might fail if the ASA does not have a return route to the host through the intermediate router (see Figure 77-4). In this case, the debugging messages show that the ping was successful, but syslog message 110001 appears, indicating a routing failure.

Figure 77-4 Ping Failure Because the ASA has No Return Route



Passing Traffic Through the ASA

After you successfully ping the ASA interfaces, make sure traffic can pass successfully through the ASA. For routed mode, this test shows that NAT is operating correctly, if configured. For transparent mode, which does not use NAT, this test confirms that the ASA is operating correctly. If the ping fails in transparent mode, contact Cisco TAC.

To ping between hosts on different interfaces, perform the following steps:

	Command	Purpose
Step 1	`access-list ICMPACL extended permit icmp any any`	Adds an access list allowing ICMP from any source host. **Note** By default, when hosts access a lower security interface, all traffic is allowed through. However, to access a higher security interface, you need the preceding access list.
Step 2	`access-group ICMPACL in interface` *`interface_name`*	Assigns the access list to each source interface. **Note** Repeat this command for each source interface.

Step 3	`class-map ICMP-CLASS`
	`match access-list ICMPACL`
	`policy-map ICMP-POLICY`
	`class ICMP-CLASS`
	`inspect icmp`
	`service-policy ICMP-POLICY global`
		Enables the ICMP inspection engine and ensure that ICMP responses may return to the source host.
		Note Alternatively, you can also apply the ICMP access list to the destination interface to allow ICMP traffic back through the ASA.

Step 4	`logging on`	Enables syslog message generation.

Ping from the host or router through the source interface to another host or router on another interface.

Repeat this step for as many interface pairs as you want to check.

If the ping succeeds, a syslog message appears to confirm the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter either the **show xlate** or **show conns** command to view this information.

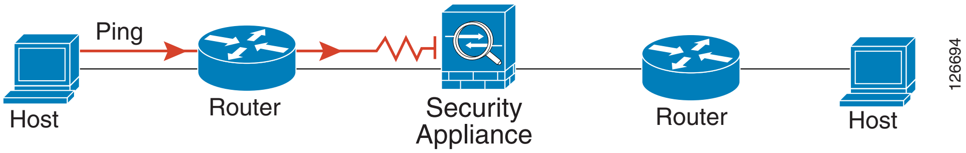
If the ping fails for transparent mode, contact Cisco TAC.

For routed mode, the ping might fail because NAT is not configured correctly (see Figure 77-5). In this case, a syslog message appears, showing that the NAT failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation, the following syslog message appears:

```
%ASA-3-106010: deny inbound icmp.
```

Note The ASA only shows ICMP debugging messages for pings to the ASA interfaces, and not for pings through the ASA to other hosts.

Figure 77-5 Ping Failure Because the ASA is Not Translating Addresses



Disabling the Test Configuration

After you complete your testing, disable the test configuration that allows ICMP to and through the ASA and that prints debugging messages. If you leave this configuration in place, it can pose a serious security risk. Debugging messages also slow the ASA performance.

To disable the test configuration, perform the following steps:

	Command	Purpose
Step 1	`no debug icmp trace`	Disables ICMP debugging messages.
Step 2	`no logging on`	Disables logging.

Step 3	`no access-list ICMPACL`	Removes the ICMPACL access list, and deletes the related **access-group** commands.
Step 4	`no service-policy ICMP-POLICY`	(Optional) Disables the ICMP inspection engine.

Determining Packet Routing with Traceroute

You can trace the route of a packet using the traceroute feature, which is accessed with the **traceroute** command. A traceroute works by sending UDP packets to a destination on an invalid port. Because the port is not valid, the routers along the way to the destination respond with an ICMP Time Exceeded Message, and report that error to the ASA.

Tracing Packets with Packet Tracer

The packet tracer tool provides packet tracing for packet sniffing and network fault isolation, as well as detailed information about the packets and how they are processed by the ASA. If a configuration command did not cause the packet to drop, the packet tracer tool provides information about the cause in an easily readable manner.

In addition, you can trace the lifespan of a packet through the ASA to see whether the packet is operating correctly with the packet tracer tool. This tool lets you do the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet, along with the CLI commands that caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

To trace packets, enter the following command:

Command	Purpose

`packet-tracer`
Example:
`hostname# packet-tracer`
`packet dropped due to bad ip header (`*`reason`*`)`
	Provides detailed information about the packets and how they are processed by the ASA. The example shows the resulting message that appears when a packet is dropped because of an invalid header validation.

Reloading the ASA

In multiple mode, you can only reload from the system execution space. To reload the ASA, enter the following command:

Command	Purpose
`reload`	Reloads the ASA.

Performing Password Recovery

This section describes how to recover passwords if you have forgotten them or you are locked out because of AAA settings, and how to disable password recovery for extra security. This section includes the following topics:

- Recovering Passwords for the ASA, page 77-7
- Disabling Password Recovery, page 77-8
- Resetting the Password on the SSM Hardware Module, page 77-9

Recovering Passwords for the ASA

To recover passwords for the ASA, perform the following steps:

Step 1 Connect to the ASA console port according to the instructions in the "Accessing the Command-Line Interface" section on page 2-4.

Step 2 Power off the ASA, and then power it on.

Step 3 After startup, press the **Escape** key when you are prompted to enter ROMMON mode.

Step 4 To update the configuration register value, enter the following command:

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

Step 5 To set the ASA to ignore the startup configuration, enter the following command:

```
rommon #1> confreg
```

The ASA displays the current configuration register value, and asks whether you want to change it:

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

Step 6 Record the current configuration register value, so you can restore it later.

Step 7 At the prompt, enter **Y** to change the value.

The ASA prompts you for new values.

Step 8 Accept the default values for all settings, except for the "disable system configuration?" value.

Step 9 At the prompt, enter **Y**.

Step 10 Reload the ASA by entering the following command:

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

The ASA loads the default configuration instead of the startup configuration.

Step 11 Access the privileged EXEC mode by entering the following command:

```
hostname# enable
```

Step 12 When prompted for the password, press **Enter**.

The password is blank.

Step 13 Load the startup configuration by entering the following command:

```
hostname# copy startup-config running-config
```

Step 14 Access the global configuration mode by entering the following command:

```
hostname# configure terminal
```

Step 15 Change the passwords, as required, in the default configuration by entering the following commands:

```
hostname(config)# password password
hostname(config)# enable password password
hostname(config)# username name password password
```

Step 16 Load the default configuration by entering the following command:

```
hostname(config)# no config-register
```

The default configuration register value is 0x1. For more information about the configuration register, see the *Cisco ASA 5500 Series Command Reference*.

Step 17 Save the new passwords to the startup configuration by entering the following command:

```
hostname(config)# copy running-config startup-config
```

Disabling Password Recovery

To disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA, enter the following command:

Command	Purpose
`no service password-recovery`	Disables password recovery.

On the ASA, the **no service password-recovery** command prevents a user from entering ROMMON mode with the configuration intact. When a user enters ROMMON mode, the ASA prompts the user to erase all Flash file systems. The user cannot enter ROMMON mode without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON mode and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to restore the system to an operating state, load a new image and a backup configuration file, if available.

The **service password-recovery** command appears in the configuration file for information only. When you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the ASA is configured to ignore the startup configuration at startup (in preparation for password recovery), then the ASA changes the setting to load the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

Resetting the Password on the SSM Hardware Module

To reset the password to the default of "cisco" on the SSM hardware module, enter the following command:

Note Make sure that the SSM hardware module is in the Up state and supports password reset.

Command	Purpose
hw-module module 1 password-reset Reset the password on module in slot 1? [confirm] **y** hostname# **y**	Where *1* is the specified slot number on the SSM hardware module. **Note** On the AIP SSM, entering this command reboots the hardware module. The module is offline until the rebooting is finished. Enter the **show module** command to monitor the module status. The AIP SSM supports this command in version 6.0 and later. On the CSC SSM, entering this command resets web services on the hardware module after the password has been reset. You may lose connection to ASDM or be logged out of the hardware module. The CSC SSM supports this command in the most recent version of 6.3, dated January 2010.

Using the ROM Monitor to Load a Software Image

This section describes how to load a software image to an ASA from the ROM monitor mode using TFTP.

To load a software image to an security appliance, perform the following steps:

Step 1 Connect to the ASA console port according to the instructions in "Accessing the Command-Line Interface" section on page 2-4.

Step 2 Power off the ASA, and then power it on.

Step 3 During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

Step 4 In ROMMOM mode, define the interface settings to the security appliance, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```

Note Be sure that the connection to the network already exists.

Step 5 To validate your settings, enter the **set** command.

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa800-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

Step 6 Ping the TFTP server by entering the **ping server** command.

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Step 7 Load the software image by entering the **tftp** command.

```
rommon #8> tftp
ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa800-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp f1/asa800-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar  5 16:00:07 MST 2007

Loading...
```

After the software image is successfully loaded, the ASA automatically exits ROMMOM mode.

Step 8 To verify that the correct software image has been loaded into the ASA, check the version in the ASA by entering the following command:

```
hostname# show version
```

Erasing the Flash File System

To erase the flash file system, perform the following steps:

Step 1 Connect to the ASA console port according to the instructions in the "Accessing the Command-Line Interface" section on page 2-4.

Step 2 Power off the ASA, and then power it on.

Step 3 During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

Step 4 To erase the file system, enter the **erase** command, which overwrites all files and erases the file system, including hidden system files.

```
rommon #1> erase [disk0: | disk1: | flash:]
```

Other Troubleshooting Tools

The ASA provides other troubleshooting tools that you can use. This section includes the following topics:

- Viewing Debugging Messages, page 77-11
- Capturing Packets, page 77-11
- Viewing the Crash Dump, page 77-11
- Coredump, page 77-11

Viewing Debugging Messages

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of less network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use. To enable debugging messages, see the **debug** commands in the *Cisco ASA 5500 Series Command Reference*.

Capturing Packets

Capturing packets is sometimes useful when troubleshooting connectivity problems or monitoring suspicious activity. We recommend contacting Cisco TAC if you want to use the packet capture feature. See the **capture** command in the *Cisco ASA 5500 Series Command Reference*.

Viewing the Crash Dump

If the ASA crashes, you can view the crash dump information. We recommend contacting Cisco TAC if you want to interpret the crash dump. See the **show crashdump** command in the *Cisco ASA 5500 Series Command Reference*.

Coredump

A coredump is a snapshot of the running program when the program has terminated abnormally, or crashed. Coredumps are used to diagnose or debug errors and save a crash for future off-site analysis. Cisco TAC may request that users enable the coredump feature to troubleshoot application or system crashes on the ASA. See the **coredump** command in the *Cisco ASA 5500 Series Command Reference*.

Common Problems

This section describes common problems with the ASA, and how you might resolve them.

Symptom The context configuration was not saved, and was lost when you reloaded.

Possible Cause You did not save each context within the context execution space. If you are configuring contexts at the command line, you did not save the current context before you changed to the next context.

Recommended Action Save each context within the context execution space using the **copy start run** command. Load the startup configuration as your active configuration. Then change the password and then enter the **copy run start** command. You cannot save contexts from the system execution space.

Symptom You cannot make a Telnet or SSH connection to the ASA interface.

Possible Cause You did not enable Telnet or SSH to the ASA.

Recommended Action Enable Telnet or SSH to the ASA according to the instructions in the "Configuring Device Access for ASDM, Telnet, or SSH" section on page 34-1.

Symptom You cannot ping the ASA interface.

Possible Cause You disabled ICMP to the ASA.

Recommended Action Enable ICMP to the ASA for your IP address using the **icmp** command.

Symptom You cannot ping through the ASA, although the access list allows it.

Possible Cause You did not enable the ICMP inspection engine or apply access lists on both the ingress and egress interfaces.

Recommended Action Because ICMP is a connectionless protocol, the ASA does not automatically allow returning traffic through. In addition to an access list on the ingress interface, you either need to apply an access list to the egress interface to allow replying traffic, or enable the ICMP inspection engine, which treats ICMP connections as stateful connections.

Symptom Traffic does not pass between two interfaces on the same security level.

Possible Cause You did not enable the feature that allows traffic to pass between interfaces at the same security level.

Recommended Action Enable this feature according to the instructions in the "Allowing Same Security Level Communication" section on page 6-30.

Symptom IPSec tunnels do not duplicate during a failover to the standby device.

Possible Cause The switch port that the ASA is plugged into is set to 10/100 instead of 1000.

Recommended Action Set the switch port that the ASA is plugged into to 1000.