Zeroization

Zeroization erases all potentially sensitive information in the router memory. This includes the erasure of the main memory, cache memories, and other memories containing packet data, NVRAM, and Flash memory. The Zeroization button on the faceplate is used to invoke zeroization. The parameters for zeroization can be configured, but zeroization cannot be invoked through the command-line interface (CLI).

Zeroization is disabled by default.

Feature History for zeroisation

Release	Modification
12.3(8)YD	This feature was introduced.
12.4(2)T	This feature was integrated into Cisco IOS Release 12.4(2)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Zeroization

- Zeroization is supported on the Cisco 3200 series routers only.
- When zeroization is enabled, the auxiliary (AUX) port should not be used for any function other than an actuator, such as a push button. There is no way to reliably ascertain whether a device connected to the AUX port might trigger zeroization. We recommend that if zeroization is enabled, no devices, with the exception of the zeroization actuator, be attached to the AUX port. There are some AUX port configuration restrictions that apply when zeroization is enabled.
- Zeroization can only be invoked and executed locally. It cannot be invoked and executed remotely through a Telnet session.
- Zeroization shuts down all network interfaces and causes zeroization of the Cisco IOS configuration and object code files, including all IP addresses on the router that are contained in volatile memory.

Information About Zeroization

Scrubbing the Router Memory

Scrubbing is defined as performing several passes through the memory areas, overwriting the memory using a separate data pattern for each pass. The data patterns used for scrubbing consist of separate passes; each pass fills the memory with the following data patterns:

- All ones (that is, 0xffff ffff)
- Alternating ones and zeroes (that is, 0xa5a5 a5a5)
- Alternating zeroes and ones (that is, 0x5a5a 5a5a)
- All zeroes (that is, 0x0000 0000)

The data patterns ensure that

- Each bit in the memory is cleared to zero and set to one at least once.
- The final state of the memory is such that all prior information is erased.

The following items in the router memory are scrubbed:

- Dual-port RAM in the CPM
- Main memory

All the main memory is scrubbed except the memory area containing a small program loop that does the actual scrubbing.

The following items in the router memory cannot be scrubbed:

- Console and AUX port UART FIFO queues. A series of characters is forced through the FIFO queues to ensure that all sensitive information in the FIFO queues is flushed.
- NVRAM, which is erased entirely.
- Flash memory file system, which is erased entirely.
- Caches, which are flushed and invalidated, eliminating all of the information. The process of scrubbing the main memory causes all cache lines to receive the scrubbing data patterns.

Note Some items cannot be completely scrubbed. For example, some devices provide a reset or invalidate of their memory, rather than providing a full data path through which the scrubbing patterns can be written upon memory.