



# CHAPTER 13

## Zeroization

---

Zeroization consists of erasing any and all potentially sensitive information in the router. This includes erasure of main memory, cache memories, and other memories containing packet data, NVRAM, and selected files in the Flash file system such as crash dumps. Zeroization is launched upon the initiation of a user command and subsequent trigger. In this document declassification and zeroization mean the same thing, and they are used interchangeably.



Note

---

Zeroization is available on only the Cisco 5930 ESR.

---

## Restrictions for Zeroization

The following restrictions apply when using zeroization on the Cisco 5930 ESR.

- When zeroization is enabled do not use the auxiliary (AUX) port 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 takes about five minutes to complete.
- 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 contained in volatile memory.

## 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.

Zeroization Command Reference 3

- 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 their memory, rather than providing a full data path through which the scrubbing patterns can be written upon memory.

---

## End User Interface

The following Zeroization (declassification) commands are supported on the Cisco 5930 ESR in Cisco IOS Release 15.2(4)GC.

- [service declassify](#), page A-69

For information about these commands, see [Appendix A, “Command Reference”](#)