CHAPTER 10

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. Zeroization is launched by taking an action. Typically, there is a button on the faceplate that invokes zeroization. The result of that action is determined by the configuration of the router. The parameters for zeroization can be configured, but zeroization cannot be invoked through the command–line interface (CLI).

Caution Zeroization is disabled by default. When zeroization is enabled, the 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 when zeroization is enabled.

Zeroization can only be invoked and executed locally. It cannot be invoked and executed remotely through a Telnet session. The time needed for zeroizing is about 5 minutes.

Some items cannot be completely scrubbed because the devices provide a *reset* or *invalidate* of the memory, rather than providing a full data path through which the scrubbing patterns can be written.

These items 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. Scrubbing is defined as performing several passes through the memory areas, overwriting the memory using a separate data pattern for each pass.

These items cannot be scrubbed:

- Console and AUX port UART FIFOs. A series of characters is forced through the FIFOs to ensure that all sensitive information in the FIFOs is flushed.
- NVRAM, which is erased entirely.
- Flash file system, which is erased entirely.
- Caches, that 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.

The data patterns used for scrubbing consist of separate passes; each pass fills the memory with the following data patterns:

- All ones (e.g. 0xffff ffff)
- Alternating ones and zeroes (e.g. 0xa5a5 a5a5)
- Alternating zeroes and ones (e.g. 0x5a5a 5a5a)
- All zeroes (e.g. 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.

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.

In addition, 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.

Note The procedures for enabling Zeroization have been left out of this document intentionally for legal reasons. Please contact your system integrator for more information.

End User Interface

The user interface consists of configuration and show commands.

service declassify command

Enter the **service declassify** command to enable the declassification function and monitor the AUX port CTS pin. Entering the **no** form of this command disables the declassification function and AUX port monitoring. If a parameter is not specified, neither the Flash file system nor the NVRAM is declassified (erased).

Syntax Description [**no**] **service declassify** {**erase-flash** | **erase-nvram** | **erase-all**}

erase-flash	(Optional) Erases all files in the Flash file system when declassification is invoked.
erase-nvram	(Optional) Erases all files in the NVRAM file system when declassification is invoked.
erase-all	(Optional) Scrubs and erases all files on the router when declassification is invoked

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
12.3(8)TD	This command was introduced.

Usage Guidelines The network interfaces are shut down when declassification is invoked.

No CLI command invokes the declassification process. Declassification is invoked by using an external signal that appears on the AUX port of the router. When declassification is complete, the ROMMON prompt appears on the console.

The output that appears on the console when declassification is initiated depends on what options have been configured. It is not possible to document exactly what appears on the screen, because of the complex interactions between the declassification process and the logging process during declassification.

Examples The following examples show the console output when declassification is invoked.

erase-all

The output on the console when the **erase-all** parameter is set resembles the following:

```
Router#service declassify erase-all

*Mar  5 17:44:28.347:
Declassification initiated...
*Mar  5 17:44:30.647: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  5 17:44:31.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to downÿ
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note If the **service declassify erase-all** is configured and the Flash file system is erased, error recovery actions must be initiated to load a bootable image on the router. The startup configuration file is also erased; the router boots from the factory default configuration the next time it is booted.

erase-flash

The output on the console when the **erase-flash** parameter is set resembles the following:

```
Router#service declassify erase-flash

*Mar  1 00:01:30.091:
Declassification initiated...
*Mar  1 00:01:34.347: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  1 00:01:35.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
```

```
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note The flash file system is erased and there will not be a bootable image for the router in the Flash file system if the **service declassify erase-flash** is configured. Error recovery actions must be initiated to load a bootable image.

The startup configuration file is not erased if the **service declassify erase-flash** is configured. When the router is booted, it is configured using its startup configuration file in NVRAM.

erase-nvram

The output on the console when the **erase-nvram** parameter is set resembles the following:

```
Router#service declassify erase-nvram
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory

rommon 1 >
```

Note If the **service declassify erase-nvram** is configured, the flash file system is not erased. The bootable image in the Flash file system remains and the router can be booted. The startup configuration file is erased; because the router has no configuration file, it boots from the default configuration.

Related Commands

Command	Description
show declassify	Displays the state of the **service declassify** command.

show declassify

Enter the **show declassify** command to display the state of the declassify function (enabled, in-progress, and so forth), and the sequence of declassification steps that will be performed.

show declassify

Command Modes Global configuration

Command History

Release	Modification
12.3(8)TD	This command was introduced.

Examples

The following is sample output for the **show declassify** command:

```
router#show declassify
Router#show declassify
    Declassify facility: Enabled=Yes  In Progress=No
    Erase flash=Yes  Erase nvram=Yes
    Obtain memory size
    Shutdown Interfaces
    Declassify Console and Aux Ports
    Erase flash
    Declassify NVRAM
    Declassify Communications Processor Module
    Declassify RAM, D-Cache, and I-Cache
```

Related Commands

Command	Description
service declassify	Invokes declassification.