CHAPTER 12

Special Debugging Problems

Soft-ICE can be a powerful tool in stand-alone mode. This chapter describes techniques for debugging system-level components using Soft-ICE in stand-alone mode. When using Soft-ICE as a stand-alone debugger, the ACTION must be set to HERE.

12.1 Loadable Device Drivers

Debugging DOS loadable device drivers requires a debugger that does not make DOS calls. Soft-ICE can be used in stand-alone mode if your debugger uses DOS.

There are two methods for debugging loadable device drivers:

1. Use the MAP command to find the location of your loadable driver. Display the device driver header to find the strategy or interrupt entry point. Setting a break point at the entry to strategy or interrupt will give you control within the device driver. Single step, or set break points further on, to continue debugging.
   Debugging the device driver initialization code requires resetting the system with the BOOT command. Use the technique stated above to set a break point within the driver code. The BOOT command will retain Soft-ICE and break points.
2. The second method requires placing special code in your driver. Do this with the 13HERE ON command (see section 5.4). Place an INT 3 opcode (CCH) in your device driver at the point where control is desired. When the INT 3 executes, control comes to Soft-ICE. You can then use an RIP command to set the instruction pointer to get around the INT 3.

If you wish to debug your initialization sequence, make sure that Soft-ICE is loaded in CONFIG.SYS prior to the driver you are trying to debug. Place the 13HERE ON command

in the INIT string in Soft-ICE.DAT. With this method you do not have to use the BOOT command.

If you are debugging your device driver symbolically or with source you must load the symbol file and the source files separately from the device driver. The symbol file and source files are loaded with the Soft-ICE program loader LDR.EXE. When LDR.EXE is used to load only the symbols and source you must use it in the form:

LDR file-name.SYM

The extension of the symbol file must be specified. See section 7.4 for more details about LDR.EXE.

After loading the symbol file and source files with LDR.EXE you must enter Soft-ICE and relocate the symbols relative to the start of your device driver. Symbols are relocated with the Soft-ICE SYMLOC command. The syntax of the SYMLOC command is:

SYMLOC segment

The segment value is obtained from the MAP command. See the description of the SYMLOC command for more details.

12.2 Boot Loaders

Debugging boot loaders or self-booting programs requires using Soft-ICE as a stand-alone debugger. You must first boot into DOS and load Soft-ICE.
The easiest method of debugging boot loaders is to set a break point at a known address within the boot loader, and then use the BOOT command to reset the system. Soft-ICE is retained throughout the boot process with the break points still set. If a known address is difficult to find an execution break point can be set at 7C0:0H before the

BOOT command. This is the address where the ROM BIOS loads the boot sector into memory.

Another method requires turning 13HERE mode on (see section 5.4). Place an INT 3 opcode (CCH) in your program at the point where control is desired. When the INT 3 executes, control comes to Soft-ICE,
You may also use both symbols and source debugging while debugging a boot loader. See the SYMLOC command for more information on how to relocate your symbols and source to the segment where your boot loader has been loaded

12.3 Interrupt Routines

Soft-ICE allows break points and single stepping within hardware interrupt service routines (timer, keyboard, etc.).
Single stepping and setting break points in interrupt service routines is allowed with Soft-ICE. You can even single step through the keyboard interrupt routine while Soft-ICE is using the keyboard for

input.
In most cases, Soft-ICE must be used as a stand-alone debugger when debugging interrupt service routines. To set a break point on the address of the interrupt service routine, use one of the following methods:

1. Use the display double command:
   DD interrupt-number * 4 L 1
   The address displayed is the address of the first instruction of the interrupt service routine. Set a execution break point on this address.
2. Use the command:
   BPINT interrupt-number

12.4 Non-DOS Operating Systems

Non-DOS real address mode operating systems can be debugged with Soft-ICE. If the operating system is not very DOS compatible you may have to load Soft-ICE under DOS, and then use the BOOT command to start the non-DOS operating system. Follow the instructions for debugging boot sequences and self-booting programs explained in section 12.2.

The MAP and WARN commands may not function properly under a non-DOS operating system, but break points and the other debugging commands will work correctly.

If debugging with symbols or source you must load symbol files and source files while still under DOS or in the DOS compatible mode of your operating system.

Page 226 is BLANK