CHAPTER 9

Back Trace Ranges

9.1 Introduction

Soft-ICE can collect instruction information in a back trace history buffer as your program executes. These instructions can then be displayed after a bug has occurred. This allows you to go back and retrace a program's action to determine the actual flow of instructions preceding a break point.

Instruction information is collected on accesses within a specified address range, rather than system wide. The ranges can be from 1 byte to 1 megabyte, so if desired, complete system information can be obtained. Using specific ranges rather than collecting all instructions is useful for two reasons:

1. The back trace history buffer is not cluttered by extraneous information that you are not interested in. For example, you may not be interested in interrupt activity and execution within MSDOS.
2. Back trace ranges degrade system performance while they are active. By limiting the range to an area that you are interested in, you can improve system performance greatly.

Soft-ICE has two methods of utilizing the instructions in the back trace history buffer:

1. The SHOW command allows you to display instructions from the back trace history buffer. You must specify how many instructions you wish to go back in the buffer.
2. The TRACE command allows you to go back and replay instructions from the back trace history buffer, This way you can see the instruction flow within the context of the surrounding program code or source code.

9.2 Using Back Trace Ranges

To use back trace ranges you must do the following:

1. Allocate a back trace history buffer of the desired size by inserting the /TRA switch on the S-ICE.EXE line in CONFIG.SYS. For example, to create a back trace buffer of 100K you might have the following line in your CONFIG.SYS file:

   ```
   DEVICE = S-ICE.EXE 100
   ```

   A back trace history buffer of 10K is allocated by default. If this is suitable for your needs you do not have to allocate a larger buffer.

   The history buffer size is only limited by the amount of extended memory available.
2. Enable back trace ranges by creating a memory range break point with the T or TW verb. For example:

   ```
   BPR 1000:0 2000:0 T
   ```

   The T and TW verbs do not cause break points instead they log instruction information that can be displayed later with the SHOW or TRACE commands.
3. Set any other break points if desired.
4. Exit from Soft-ICE with the X command.
5. After a break point has occurred, or you have popped Soft-ICE up with the hot key, you can display instructions in the buffer with the SHOW command. For example, to go back 50 instructions in the buffer and display instructions type:

   ```
   SHOW 50
   ```

6. To replay a series of instructions you must first enter trace simulation mode with the TRACE command. To begin replaying the sequence of instructions starting back 50 in the buffer type:

   ```
   TRACE 50
   ```

7. After you have entered trace simulation mode, you can trace through the sequence of instructions by using the XT, XP, or XG commands. This allows you to re-enact the program flow. For example, you can single step through the sequence of instructions in the buffer, starting at the instruction specified by the TRACE command, by typing:

   ```
   XT
   ```

```
 XT
.
 .
.
XT
```

The XT command single steps through the back trace history buffer. The XP command program steps through the back trace history buffer. The XG command goes to an address in the back trace history buffer.

8. To exit from trace simulation mode type:

   ```
   TRACE OFF
   ```

9. To reset the back trace history buffer, use the X command.

9.3 Special Notes

While in trace simulation mode, most Soft-ICE commands work as normal, including displaying the memory map, and displaying and editing data. The exceptions are:

1. Register information is not logged in the back trace history buffer, so the register values do not change as you trace through the buffer, except for CS and IP.
2. Commands that normally exit from Soft-ICE do not work while in trace simulation mode. These are X, T, P, G, EXIT.

As you peruse instructions from the back trace history buffer with the SHOW and TRACE commands, you may notice peculiarities in instruction execution. These are caused by jumps in and out of the specified range. These usually occur at jumps, calls, returns and entry points.

When you have a hang problem or other difficult bug that requires back trace ranges, you must often use very large ranges in order to narrow the scope of the problem. Once you have a better idea of the specific problem area, you go to smaller ranges.

Large back trace ranges are often very slow. When using large ranges you are usually trying to get a general idea where the problem is. Soft-ICE has a special 'COARSE' mode for doing large ranges. This speeds up the ranges a factor of three or more, but limits the amount of instructions in the history buffer.

Coarse mode only collects instructions that do a memory write within the specified range. As you are replaying instructions with trace simulation mode after a 'coarse' range you will notice that the flow skips around rather than sequentially executing instructions.

Coarse ranges work best for large ranges and tend to be less effective for small ranges.

To enable a 'coarse' back trace range, use the BPR command with the TW verb instead of the T verb. For example:

```
 BPR 1000:0 2000:0 TW
```

For further information on back trace ranges see the command descriptions for:

SHOW, TRACE, XT, XP, XG, XRSET, BPR