What is Minidump?

?Mini-Dump is a user mode post mortem debugging technology that allows engineers to 'replay' exceptions that occurred on a customer system as if they were running locally. ?With just a MiniDump file (.mdmp) and a properly configured symbol store and source code, a post-mortem can be replayed. All of the relevant binaries, associated symbols and source code will be loaded on the fly.

Who has introduced Minidump Technology ?

?Mini-Dump technology was first introduced by Microsoft circa Windows 2000.

Which Release of ICM used Minidump Technology ?

?7.0 will be first release to leverage this technology.

Which was Technology used before the use of Minidump?

?Dr. Watson.

What is Dr.Watson ?

http://cisco.com/en/US/partner/products/sw/custcosw/ps1001/products_tech_note09186a0080153ffa.shtml

Why did Cisco Embrace Minidump Technology from ICM 7.0 rather than Dr.Watson ?

?Dr. Watson is limited and very old technology. ?Dr. Watson cannot decode the new Visual Studio .NET 2003 symbol files. ?Microsoft dropped support for embedding COFF symbols in binaries after Visual Studio 6.0. ?MiniDump is fully configurable by the application as to the amount of information captured in a dump. ?Custom user-defined streams can be added to a MiniDump (not yet implemented in ICM). ?File management is defined by the application. ?Dr. Watson can create CrashDumps (.dmp), that also can be used similarly to a MiniDump, but it is has limitations.

How is Minidump Configured ?

Checklists to be followed by TAC before escalating the case to CCBU for Minidump analysis.

1.TAC need to provide callflow and versions of ICM with SR/ES installed

```
( if any ).
```

2.TAC needs to collect Logs of Matching Time stamps at the time

```
Minidump was generated.
```

3.TAC need to Collect the following files :- a) If router is crashing and generating a Mini Dump, Collect the Following files :- ?Router Mini Dump files (.mdmp files) ?router.exe (under icm\bin) ?router.pdb (under icm\bin)

b) If Logger process is crashing and generating a Mini Dump, Collect the Following files :-

?Logger Minidump files (.mdmp files) ?.exe file (under icm\bin) ?.PDB file (under icm\bin)

c) If CTIOS Server is crashing and generating a Mini Dump, Collect the Following files :-

?CTIOS Minidump files (.mdmp files) ?ctiosservernode.exe (under icm\ctios_bin) ?ctiosservernode.pdb (under icm\ctios_bin)

d) If OPC Process is crashing and generating a Mini Dump, Collect the Following files :-

?OPC Minidump files (.mdmp files) ?opc.exe (under icm\bin) ?opc.pdb (under icm\bin)

e) If PIM process is crashing and generating a Mini Dump, Collect the Following files :-

?PIM Minidump files ?.exe file (under icm\bin depending on type of PIM) ?.PDB file (under icm\bin depending on type of PIM)

f) If NIC process is crashing and generating a Mini Dump, Collect the Following files :-

?NIC Minidump files ?.exe file (under icm\bin) ?.PDB file (under icm\bin)

3) Here is a Sample example of how to search for known cases/defects when a process crashes generating a Minidump.

```
Logs show the following:
15:09:32:132 pg12A-opc Trace: ConfirmInvocation - Fail to find the
Invocation Object by InvokeID 0xf000136b
15:09:32:163 pg12A-opc Trace: ConfirmInvocation - Fail to find the
Invocation Object by InvokeID 0xf000136c
15:09:32:163 pg12A-opc Trace: ConfirmInvocation - Fail to find the
Invocation Object by InvokeID 0xf000136d
15:09:32:163 pg12A-opc Trace: ConfirmInvocation - Fail to find theInvocation Object by InvokeI
15:09:32:382 pg12A-opc Trace: CExceptionHandlerEx::GenerateMiniDump - A
Mini Dump File is available at logfiles\opc.exe_20070726150932351.mdmp
15:09:32:663 pg12A-opc Unhandled Exception: Exception code: C0000005
ACCESS_VIOLATION
 Fault address:  004E9FA1 01:000E8FA1 C:\icm\bin\opc.exe
 Registers:
EAX:00000000
EBX:00000000
ECX:01EC8008
EDX:01ED1C38
ESI:0000002C
EDI:0472CD98
CS:EIP:001B:004E9FA1
SS:ESP:0023:0012E454  EBP:0068B594
DS:0023  ES:0023  FS:003B  GS:0000
Flags:00010202
 Call stack:
Address   Frame
004E9FA1  0012E45C  Peripheral::HashInActiveCall+41004EBABB  0012E46C  Peripheral::AddActiveCa
00452139  0012E620  Call::ConnectionCleared+21D9
0044FFFD  0012E7CC  Call::ConnectionCleared+9D
00466865  0012FDF4  CSTAConnectionClearedEvent+315
004605EE  0012FE04  CallEventControl::Initialize+46E
0050485D  0012FE20
CNFGMSGGetConfigPermissionInd::SetConfigSequenceNumber+AD
00504F4F  0012FE3C  ProcessPIMMsgs+17F
00552E44  0012FE94  MDSGetHandle+154
00555EFD  0012FEAC  MDSStartClient+2AD
00491F0C  0012FEB0  OPCInput::MDSInput+FC
00491F55  0012FEC8  OPCInput::ProcessInput+35
004924DF  0012FEF4  OPCInput::StartInput+1BF
```

```
004A30C2  0012FF24  OPCMain::Execute+4A2
0054430A  0012FF38  Reader::SingleCommand+CA
004A2A8E  0012FF60  main+8E
005C823B  0012FFC0  mainCRTStartup+143
77E523E5  0012FFF0  IsProcessorFeaturePresent+9E.
* *
```

Tips for Troubleshooting :-

1.Do a Topic search (topic.cisco.com)on the following keywords : "OPC assert Peripheral::HashInActiveCall" 2.Follow the resolution summary if a matching case/defect is found. Else escalate to CCBU.