Microsoft Product Support Services

Support WebCasts

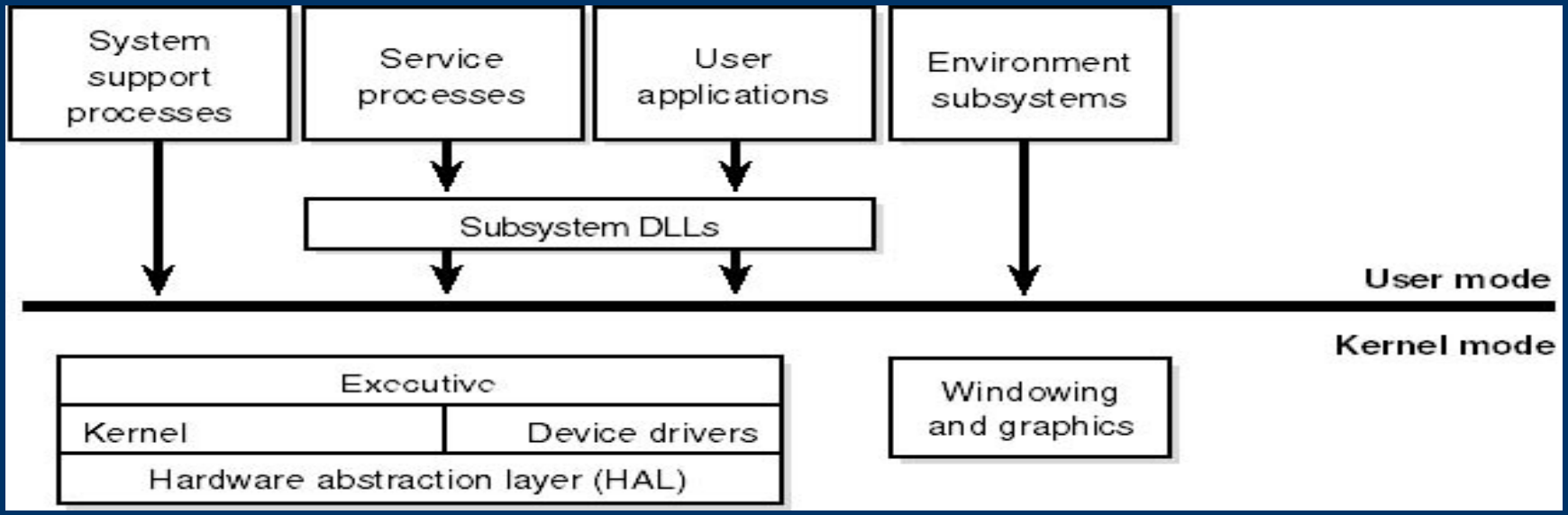
Basic STOP Error (Blue Screen) Troubleshooting

Doug Allen
Support Professional
PSS Premier Setup Team
Microsoft Corporation

OS Architecture – Background

- Divided into two main sections
  - Kernel mode – high-privilege, direct access to hardware, memory, HAL, MicroKernel, NT Executive Services
  - User mode – low privilege, no direct access to hardware, uses APIs to request system resources, environment, and integrated subsystems

OS Architecture – Background (2)



Why Do STOP Screens Happen?

- Services, applications, or device drivers are faulty or incompatible
- Hardware problems
- Disk or file system corruption
- Firmware or BIOS outdated or incompatible
- Viruses

When Do STOP Screens Happen?

- Four categories
  - Short startup period (phase four of the boot sequence)
  - Software condition detected by the CPU
  - Hardware malfunction detected by the CPU
  - All the rest of the STOP codes

Windows NT 4.0 STOP Screen Breakdown

- Five sections
  - Section 1 – Debug port status info
  - Section 2 – Bug check info
  - Section 3 – Driver information loaded in memory
  - Section 4 – Kernel build number and stack dump
  - Section 5 – Debug port info

Windows NT 4.0 STOP Screen Breakdown (2)

- Debug port status info – much like Snd/Rcv indicators of a modem
- Bug check info – contains numbers in hex with symbolic string error code, and four bug check parameters
- Driver information loaded in memory
  - First column – load base address
  - Second column – time/date stamp in hex
  - Third column – names all drivers

Windows NT 4.0 STOP Screen Breakdown (3)

- Kernel build number and stack dump – version of Ntoskrnl.exe.
  - Rest is the stack dump showing range of addresses that pertain to failed module
- Debug port info – confirmation of COM parameters
  - May also show if the Memory.dmp file is being created

Windows 2000 STOP Screen Breakdown

- Three sections
  - Section 1 – bug check info
  - Section 2 – recommended user action
  - Section 3 – debug port info

Windows 2000 STOP Screen Breakdown (2)

- Bug check info – contains numbers in hex with symbolic string error code, and four bugcheck parameters
- Recommended user action – provides a list of suggestions for recovering from the error
- Debug port info – much like Snd/Rcv indicators of a modem

The Memory.dmp File

- Contains information about the computer at the time of the crash
- Creates a Memory.dmp every time
- Generates a STOP error if configured
- Used with debugging process to determine root cause of crash
- Verifies integrity using the Dumpchk.exe utility from the Windows NT® or Windows® 2000 retail CD-ROM

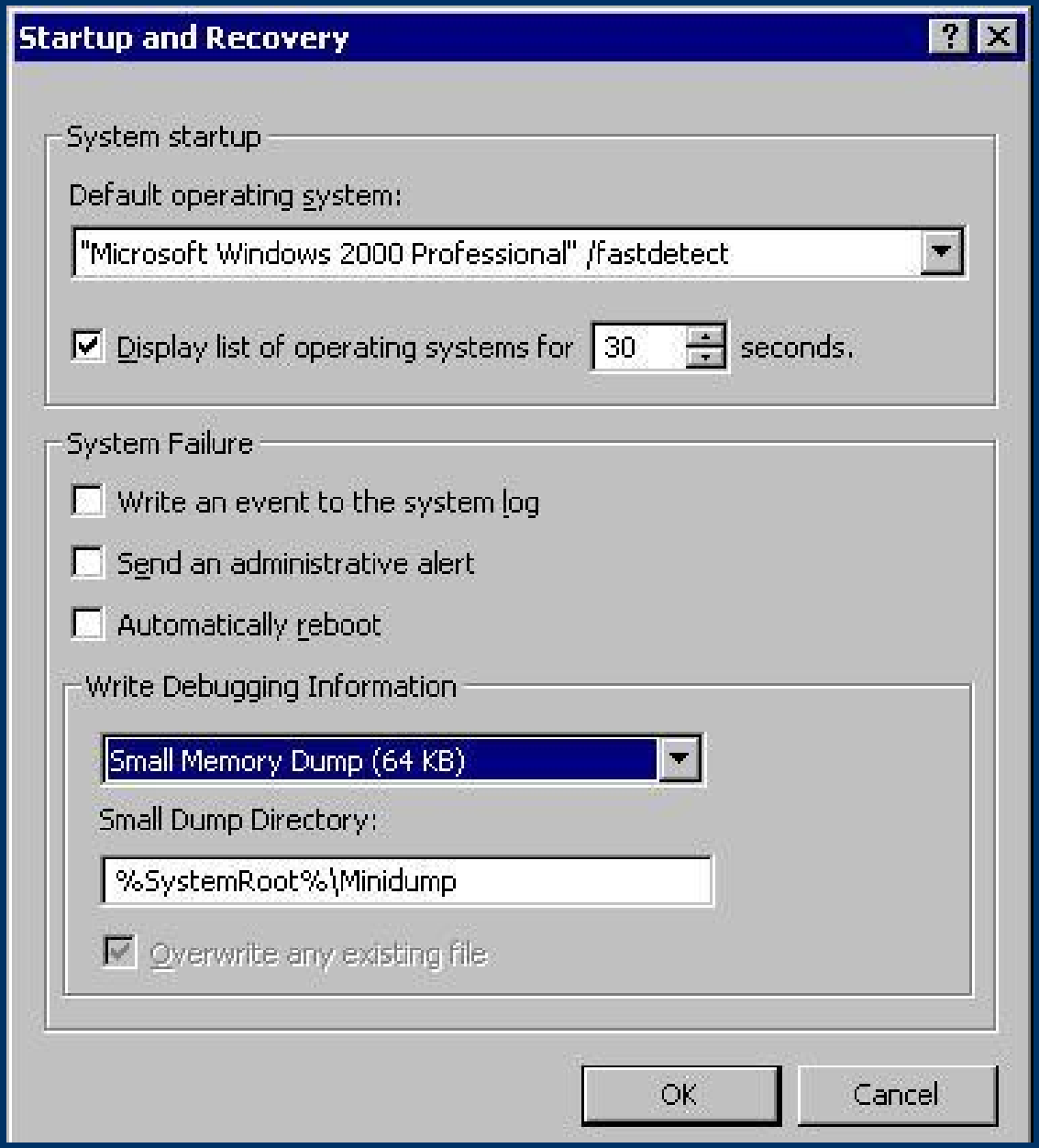
Changes with Windows 2000 Memory.dmp Options

- Mini dump (64 KB)
- Kernel only dump
- Complete dump

Memory.dmp Creation Conditions

- Valid Pagefile at least same size as amount of physical RAM plus 12 MB, located on %SYSTEMROOT% partition
- Enough free space to write the Memory.dmp file

Memory.dmp Creation Conditions (2)



Memory.dmp Creation Conditions (3)

- Must be configured to write the dump file
  - Configuration options are in the Startup Shutdown tab in the GUI, or in the registry at:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
- If the system stops responding, you can force a Memory.dmp to be created

Forcing the Creation of a Memory Dump

- Requires two configurations to be made
  - Must be set to create a Memory.dmp in the Startup Recovery options
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\i8042prt\Parameters/, set a key named CrashOnCtrlScroll equal to REG_DWORD 0x1
- To force the dump, hold down the *right* CTRL key while pressing the SCROLL LOCK key twice.

Most Common STOP Codes

- **STOP 0x0000000A IRQL_NOT_LESS_EQUAL**
  - **Caused by a kernel-mode process that tried to access portion of memory at an IRQL that was too high**
  - **Fourth parameter most important**
  - **Usually caused by buggy device drivers, or services from backup utilities or virus scanners**

Most Common STOP Codes (2)

- **STOP 0x0000001E KMODE_EXCEPTION_NOT_HANDLED**
  - Caused when a kernel-mode process tries to execute an illegal or unknown processor instruction
  - Second parameter is most important; it is the address where the exception occurred
  - If Win32k.sys is the referenced driver, check third-party remote control applications

Most Common STOP Codes (3)

- **STOP 0x00000024 NTFS_FILE_SYSTEM**
  - Caused by a problem that occurred in Ntfs.sys
  - First parameter most important
  - Usually caused by disk corruption, disk defragmenters, or (in rare cases) creating a partition larger than 7 GB on a Services for Macintosh volume with a large number of files

Most Common STOP Codes (4)

- **STOP 0x0000002E DATA_BUS_ERROR**
  - Caused by a parity error in the system memory
  - Almost always caused by hardware problems being a configuration issue, defective hardware, incompatible hardware
  - If physical RAM was recently added to the system, remove it and see if the error still occurs
  - If the error persists, try disabling memory caching in the BIOS

Most Common STOP Codes (5)

- **STOP 0x00000050 PAGE_FAULT_IN_NONPAGED_AREA**
  - Caused when requested data is not found in memory; the system checks the page file, but the missing data is identified as unable to be written to the page file
  - First parameter indicates virtual address that caused the fault
  - If this occurs on a Terminal Server, check for third-party printer drivers

Most Common STOP Codes (6)

- **STOP 0x0000007B INACCESSIBLE_BOOT_DEVICE**
  - Caused when Windows lost access to the system partition during the Startup process
  - Cannot be debugged because it usually occurs before the debugger is loaded
  - This can be caused by: an incorrect driver for a SCSI, RAID, or UDMA IDE controller; incorrect ARC path in the Boot.ini; or a failed boot device
  - During install, press F6 at prompt to install third-party Mass Storage drivers

Most Common STOP Codes (7)

- **STOP 0x0000007F UNEXPECTED_KERNEL_MODE_TRAP**
  - **Caused when the CPU generates an error that the kernel does not catch**
  - **First parameter most important (see Knowledge Base article Q137539 for details)**
  - **Usually hardware, especially RAM**
  - **Disable sync negotiation in SCSI BIOS; check SCSI termination**
  - **Can also be caused by CPU over-clocking**

Most Common STOP Codes (8)

- **STOP 0x0000009F DRIVER_POWER_STATE_FAILURE**
  - Caused when drivers do not handle power state transition requests properly
  - Most frequently when shutting down or resuming from standby or hibernation mode
  - Check CD writing software, applications that attempt to catch crashes, or other similar applications
  - Check power management compatibility and settings

Most Common STOP Codes (9)

- **STOP 0x000000D1**
  DRIVER_IRQL_NOT_LESS_OR_EQUAL
  - Occurs when the system attempts to access pageable memory at a process IRQL that is too high
  - Fourth parameter is most important, which is the address that referenced the memory
  - Very similar to STOP 0xA
  - Same troubleshooting as a STOP 0xA

Most Common STOP Codes (10)

- **STOP 0xC000021A STATUS_SYSTEM_PROCESS_TERMINATED**
  - Caused when the user-mode subsystem (Winlogon or CSRSS) is fatally compromised and security cannot be guaranteed
  - One of few user-mode errors that can bring down a machine
  - Most common causes are third-party applications or mismatched system files
  - Sfc/Scannow

Troubleshooting STOP Screens

- Emergency Repair Disk (ERD)
- Windows NT boot disk (see Q301680)
- Parallel installation of the OS
- Windows NT 4.0 and Windows 2000
  - VGA mode
  - Last known good
- Windows 2000 Only
  - Safe mode
  - Recovery console

Troubleshooting STOP Screens (2)

- System and Application Event logs
- Verify the latest service pack is installed by running the Winver command
- Virus check the system with the latest virus definitions
- Chkdsk/f/r
- Run the MPSReports utility, provided by a Microsoft Support Professional

Using the Recovery Console

- Allows command-line access to the boot partition or simple volume
- Cannot be pre-staged with Sysprep
- Is very useful to disable or enable services and devices, replace files, display modify disk/partition info, and replace the master boot record or the boot sector
- Q229716 lists all valid commands

Preventative Maintenance for STOP Screens

- Always test your drivers before installing in production
- Check the HCL before installing new hardware to verify compatibility
- For Windows 2000, install digitally signed drivers whenever possible
- Always make a new ERD after any major system change

Kernel and User Mode Debugging

- Used to determine root cause
- Should be reserved for more advanced users
- Symbols and debugging tools can be downloaded from: http://www.microsoft.com/ddk/debugging/ Symbols are also on the retail CD-ROM of the OS or service pack
- See Knowledge Base article Q148658 for more information about debugging

Additional Resources

- Windows NT 4.0 and Windows 2000 Resource Kits
- http://www.microsoft.com/ddk/
- http://www.microsoft.com/windows2000/techinfo/reskit/WebResources/default.asp
- Hardware Compatibility List
- Microsoft TechNet, MSDN®
- Microsoft Knowledge Base

Microsoft Product Support Services

Support WebCasts

Where do you want to go today?®

Microsoft