NetWare ADVISOR SUMMIT

ASN301

# A Preventative Approach to Resolving Critical Server Issues

Version 2.0 - Last revision 9/27/04

**Allan Hurst**
*Technical Principal*
KIS Computer Center
Newark, California

**Dirk A. D. Smith**
*President*
Alexander LAN, Inc.
Nashua, New Hampshire

AdvisorEvents.com

# Housekeeping

- Cell phones, pagers, Treos, Blackberries on stun, please. No noise is good noise. (Don't *make* one of us come down there; make 'em silent!)
- If you have a question, raise your hand. We'll try to answer on the fly. (We *may* ask you to be patient if it's something We're going to talk about shortly.)
- It's OK to have fun in here. Honest.
- *Please* fill out your evaluation forms. This session was created based on evalutions from prior Advisor events.

# Who are we?

## Allan Hurst / KIS Computer Center

- Spends his time fixing weird (often catastrophic) problems on enterprise and corporate networks.

Favorite Quote:

"It's never done THAT before!"

## Dirk Smith / Alexander LAN, Inc.

- Creator of the Alexander SPK which automates recovery and diagnostics of system crashes.

Favorite Quote:

"It's been really hard to login since I unloaded ETHERTSM.NLM."

# Who are you?

- This session is designed for network administrators who are responsible for installing and/or maintaining NetWare or Windows servers running Novell products…

  …because if you don't prevent this stuff from happening:

```
Abend on P00: Page Fault Processor Exception (Error code 00000000)
    OS version: Novell NetWare 5.60  August 18, 2001

...Debug symbols are enabled!
    Running Process: ABEND.NLM        1 Process
    Stack: 00 00 00 00 80 54 B0 D3 7C D1 AC D3 00 97 B0 D3
           00 00 00 00 E8 03 00 00 00 00 00 00 00 04 04
           31 00 00 00 00 97 B0 D3 00 00 00 00 00 00 00 00

Additional Information:
The CPU encountered a problem executing code in LIBC.NLM.  The problem may be
in that module or in data passed to that module by a process owned by
ABEND.NLM.

Press:
  "S"  to suspend the running process and update the ABEND.LOG file.
  "Y"  to copy diagnostic image to disk (COREDUMP).
  "X"  to update ABEND.LOG and then exit.

Writing diagnostic core dump to: C:\COREDUMP.IMG
(Press ESC to cancel)

  Writing page 165 of 261989  (normal: 90, phanton: 75)
```

- … you'll have to update one of these:

**THOMAS C. BURRELL, MCSE, CNE, CCNA**
5687 Brookstone Drive
Chicago, IL 60601
Phone: (555) 786-8083 ▪ Email: tom@emailaddress.com

**INFORMATION SYSTEMS DIRECTOR / NETWORK SERVICES MANAGER**
**Proven Technical & Management Expertise in a Career Spanning 15+ Years**

Technically sophisticated and business-savvy management professional with a pioneering career reflecting strong leadership qualifications coupled with "hands-on" IS and networking expertise. Maintain focus on achieving bottom-line results while formulating and implementing advanced technology and business solutions to meet a diversity of needs. Superior record of delivering simultaneous large-scale, mission-critical projects on time and under budget. Team-based management style and excellent interpersonal/communication skills.

***IT Strategic Planning / Business Solutions / Team Leadership / Budgeting / Project Management***
***Capital Expenditure Planning / Contract Negotiations / Vendor Relations***

**Professional Experience**

**INFORMATION SYSTEMS MANAGER**, Clinic Health System, Chicago, IL **1993 - Present**

Recruited to upgrade and replace obsolete technologies at this world-class health care organization with more than 2000 users in 15 remote locations. Hire, train, develop, and lead a 20-person technical team. Manage a $2 million capital budget and $1.2 million operating budget. Scope of position is expansive and includes departmental direction and full design, installation, engineering, implementation, support, training, administration, and management authority for:

- LAN/WAN Network Services
- 24x7 Data Center Computer Operations
- Applications Systems
- Web/Internet Design & Operations
- PC Desktop Systems
- UNIX Systems Administration
- Database Administration
- Help Desk Operations

Spearheaded transition from outdated organization-wide and departmental technologies to highly functional, streamlined, and cost-effective client-server technologies and business solutions that have dramatically improved efficiency, decreased expenses, and optimized data integrity and safety.

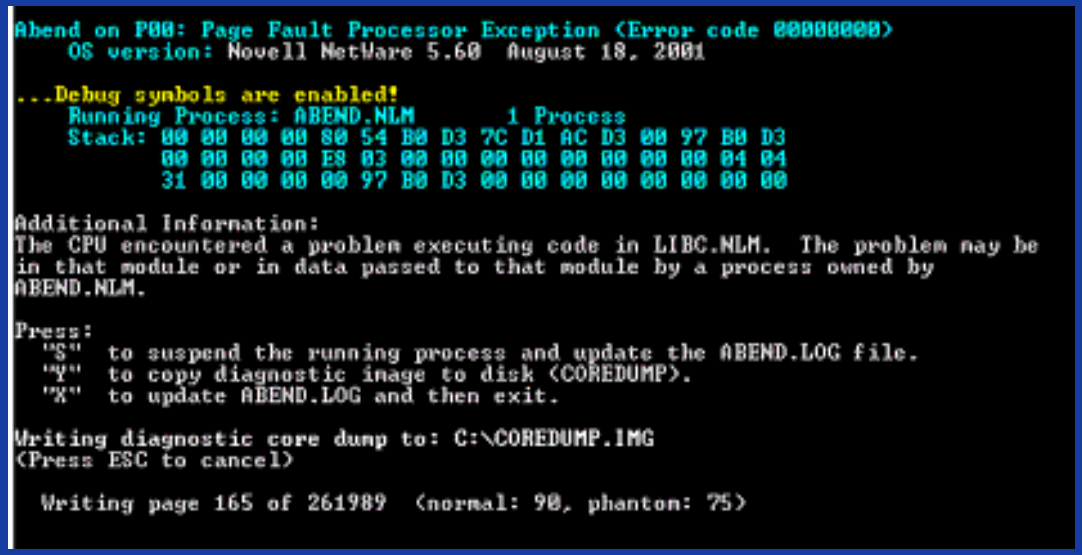
**Key Projects & Achievements:**

- Directed design and installation of the complete $8 million LAN/WAN infrastructure. Utilized state-of-the-art technologies to provide network connectivity of disparate Mainframe, AS400, UNIX, Windows NT, Novell, and PC systems.
- Completed, in just 8 months -- 22 months ahead of schedule -- a complex $15 million project forecasted to take 2.5 years and involving replacement of more than 30 systems.
- Delivered $2 million in cost savings through aggressive negotiation of contracts and pricing on a budgeted $10 million for hardware/software purchases and consulting services.
- Saved more than $1.2 million in technical consulting fees by negotiating complimentary network design services from vendors.
- Performed the work of 3 full-time equivalents, slashing labor expenses substantially by expanding personal responsibility to include UNIX, network, and database administration.
- Decreased inventory, application pricing, and licensing expenses $750K by establishing standardization for applications, PC desktops, and networking systems.
- Defused and resolved long-standing conflicts and department problems; elevated morale and decreased high employee turnover rates, achieving the best retention rate in the company.

# Why are we all here today?

- As system administrators we need to know:
  1. How to prevent crashes

     *and since they're gonna crash anyway…*
  2. How to diagnose crashes
- (If you're reading this text, you're scaring us. We can't even read this small on the laptop screen.)



# Interlude: "A funny thing happened on the way to the summit…"

# Crashes Cost Money.

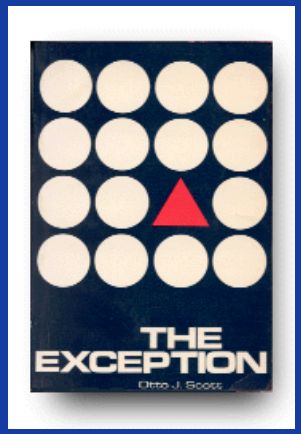
- What does a crash <u>really</u> cost your company?
- The per-hour cost of downtime is a lot higher than you may think.
- Consider a company of 100 people being paid an average of $30,000/year. That's 100 x $15/hour = $1,500/hour downtime cost! (And that's just salary, not including payroll taxes or the cost of lost business.)
- ***Many companies lose <u>MILLIONS</u> of $ per hour in lost business…***

# "Stuff" Happens.

- The best way to handle disasters?
- Prevent them from happening in the first place!
- Know how to recover from what you can't prevent.
- These techniques apply to both NetWare and Windows platforms for eDirectory.
- *Prevention is always cheaper than recovery.*

# What causes crashes?

1. Processor Exception Abends*
2. Software Exception Abends
3. Hardware Abends
4. CPU Hog Abends

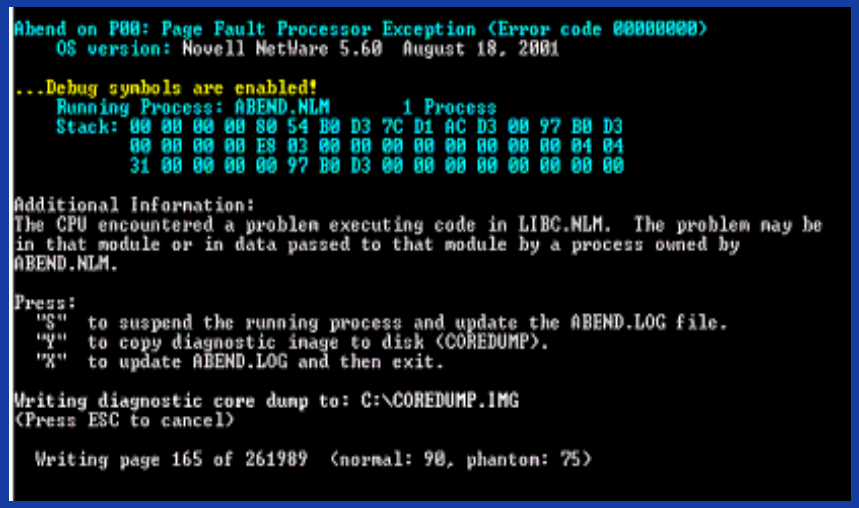



* "ABEND" = from "**AB**normal **END** of program", ie: crash. This term dates back to the first computer language compilers, long before the advent of NetWare.

# 1. "Processor Exception" Abends

Abends detected by the **CPU** are called processor exceptions.

- These always include the words "processor exception" in the error message. E.G., "Abend: Page Fault *Processor Exception*."
- Occurs when the processor encounters an invalid address or machine instruction.




- Abend message displays additional information about the abend, including the process running at the time of the abend.
- If the running process is an Interrupt Service Routine (ISR), then the problem is usually caused by a LAN or disk driver. Sometimes it can be caused by a hardware problem.

# 2. “Software Exception” Abends

Abends detected by **NetWare** are called “software exceptions”

- Abends are NetWare's way of ensuring data integrity.
- NetWare continually monitors server activities to ensure proper operation.
- When NetWare detects a condition that threatens data integrity (such as an invalid parameter being passed in a function call or certain hardware errors), it halts the active process and displays an "Abend" message on the screen (or the Alexander SPK gathers a diagnostic Crash File).
- To troubleshoot a software exception, *simplify the server* by removing software components. If the server’s stable when everything’s been removed … reload modules one at a time until the problem reoccurs.

# 3. Hardware Abends

Hardware abends are either “non-maskable interrupt” (NMI) or “machine check” errors.
**There are two kinds of NMI error messages:**

1. "Abend: NMI parity error generated by IO check."

   *The source of an IO check abend could be anywhere in the server.*

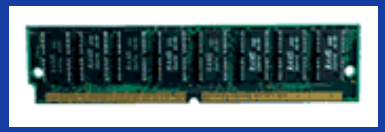
2. "Abend: NMI parity error generated by system board."

   *The source of a system board abend could be anywhere in the system, but is most likely to be in the system board or its memory.*

# 3. More on Hardware Abends…

- If your server experiences a hardware abend, run any diagnostic programs your hardware vendors provides to help locate the source of the problem.
- Try swapping hardware components to see whether the problem disappears when a particular component is replaced. Swap components in this order:

1. Memory



2. Power supply

3. System board

# 4. CPU Hog Abends

- CPU Hog abends occur when a process won't release control of the CPU within a certain period.
- This time is specified by the NetWare parameter "CPU Hog Timeout Amount ="
- When this happens, the Abend process suspends the "hog" thread.

Option 1: Try giving it more time (by setting the CPU Hog parameter to "0", then changing it back).

Option 2: Try removing the offending module, and see if that fixes the problem.

# Other Categories of server crashes

Soft Crashes … are when the OS can be prevented from needing to crash just by suspending a process and/or module.

- **In NetWare installations without the SPK**, you'll see a console prompt starting with "<*n*>", where "n" is how many abends have occurred.

  (If "*n*" is a high number your server is having a bad day.)

  Services of the suspended thread owner(s) are lost until the server's restarted.

- **In installations with the SPK**, there'll be an Edna (SPK) screen offering you the option of unloading the culprit module, cleaning up the resources, and reloading the module if you like.

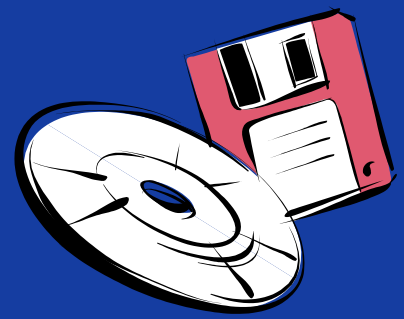
  This is useful when a module might have only been corrupted in memory, so reloading it from disk would be OK.

Hard Crashes

When nothing can prevent the system from crashing and it will have to be fully restarted to regain its services

# What are the major causes of server crashes?

- SOFTWARE
  95% of system crashes are software generated!
- Most crashes are repeat crashes.
  - This applies to servers *and* PCs
- The OS is rarely at fault (any OS!) It is usually a module from a 3rd party vendor.
- If the OS appears guilty, probably he was simply executing bad instructions passed by a 3rd party module.



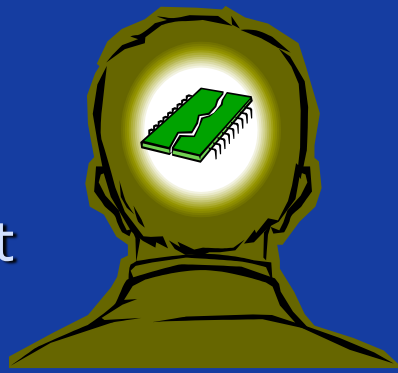
# Crashes can be very public…

# Prevention 101: Use "decent" hardware

## Brand Names Count. (Yes, really.)


- Avoid "death clones" for production machines.
- Clone components change too rapidly to find again.
  (brand-name components are usually stocked for several years)
- Clone servers are certified only at the component level.
- Avoid servers that are glorified workstations.
  (Vendors: You know who you are. Stop it!)
- Use Novell/Microsoft certified platforms only. (Please.)
- Examples of "Brand Name" servers that have worked for us:
  Compaq/HP, IBM, Dell
- REAL servers are …
  - Built entirely from components intended for 7x24 use for 3 years or more
  - Optimized for high performance/throughput as a single machine
  - Certified as a cohesive unit, NOT as individual components
- Factory-Built or Assemble It Yourself Onsite?
  - Factory-built servers still require a systems check.
  - "DIY" servers take more time, but you're certain of the result.

# Prevention 101: Add Enough Memory



- Allan's RAM Rule #1:

  "If a NetWare or Windows server will use Java, start at 1GB."

- Allan's RAM Rule #2:

  "If a server will use NetWare 6.5 or Windows 2003, start it at **2**GB."

- Allan's RAM Rule #3:

  "There is No Such Thing as `Too Much' Server Memory."

  (The old, "too much memory" rule last applied to NetWare **2.x**!)

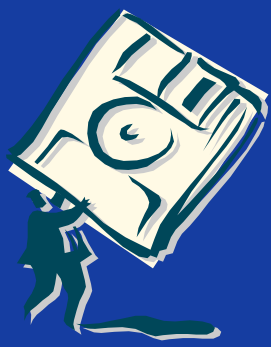
# Prevention 101: Get An Extended Warranty

Caveat Emptor: Always buy the manufacturer's extended warranty…it's *not* a bogus add-on.

- "Out of the box" warranties promise on-site service in one business day, with a dangerous caveat: "…or best effort"
- The average difference between an out-of-box warranty call and a 7x24x4 hour contract call? 3-6 business days!
- Most manufacturers maintain separate stocks of spare parts for "contract" and "non-contract" customers.
- Buy a 7x24x4 hour response onsite warranty that will last at 3 (or more) years. It's a lot cheaper than having a server down with bad hardware for one or more day(s).
- Most warranty uplifts cover only components INSIDE the server box. External systems such as tape drives or storage arrays need their own extended warranties.

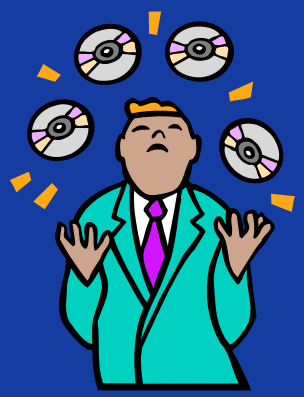
# Prevention 102: Build 'em right the first time.

- Don't use third-party components unless you're adding functionality the server manufacturer can't provide. (E.G., HBA for a SAN, special NIC, etc.)
- After building the server, upgrade firmware on ALL components before loading any software.
- Configure and burn in server hardware at least 24 hours before you start loading software.
- Download the latest drivers (NIC, disk, tape, etc.) to floppy disk or CD-R before loading the OS.



# Prevention 102: Build 'em right the first time.

- Many people have been bitten on new installs and upgrades by early "press versions" of OS CDs.
- "Pre-patched" NetWare CD-ROM images are downloadable from http://support.novell.com Use these to configure servers whenever possible. Less time, less work.
- If you can't install from a pre-patched CD, have the latest OS patch nearby on CD before you start installation.
- Don't forget to create CDs with patches or updates for other components you may need, such as newer versions of eDirectory™, iManager™, or eGuide™.
- Copy updated and third-party NIC, disk, and other drivers to C:\NWUPDATE before starting the NetWare installation or upgrade, and NetWare will "find and grab" the updated drive automatically.



# Prevention 102: Build 'em right the first time.

## Use a UPS with auto-shutdown software

- You spent HOW much on the server, and you can't bother to protect it from a 2-second brownout?
- Either use a small UPS for each server, or one large UPS for several … but each server has to have a connection back to the UPS and have auto-shutdown software loaded.

## Configure the OS with as few features as needed

- Try to NOT load every feature of the OS unless you need it
- Get the base OS working first
- Add bells and whistles later

## Document the final configuration

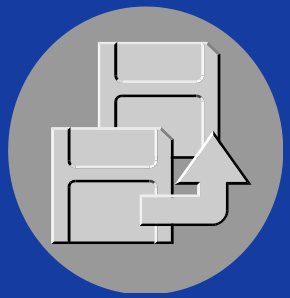
- When it's working just as you want it, use config.nlm (load config /ds) to write a config.txt file, and save it somewhere not on the server.

# Interlude: Commercial break (Survey & Giveaway)

# Prevention 103: Plan for recovery

Back up the DOS boot partition. This can cut as much as an hour from your disaster recovery time.

- Use a parallel port ZIP drive (if your server still has a parallel port)
- Load DOSFAT.NSS (NW6) and copy down to a writable CD.
- Update your DOS partition backup every time you patch the server!
- If you're running mirrored drives, don't forget to manually synchronize the DOS boot partitions on each drive.
- Copy the server's config.txt file to the same place as your DOS boot partition backup –or- keep it handy on floppy (or printed out in your network documentation binder). You'll be glad you have it when you have to rebuild the server from scratch, and don't recall what sizes each volume was or what name spaces were loaded!



# Prevention 103: Plan for recovery

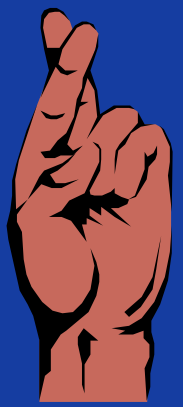
Get your "recovery kit" ready before deploying server!

- If you configured your server manually … have a boot floppy handy which contains the same version of DOS (MS-DOS/DR-DOS) as was used to create the server. (If you installed by booting from a NetWare OS CD or a NetWare license disk, have a copy of that in the kit.)
- A floppy with the correct CD-ROM and ZIP drivers on it. (Could be the same as your boot floppy.)
- A ZIP cartridge or CD-R containing a backup of the server boot partition.
- Your NetWare OS CD (pre-patched if that's what you used originally, or pre-patched to the current level).
- Copies of your NetWare license diskette(s)
- A CD-ROM containing the OS patches matching the patch level of the DOS boot partition (if not using a pre-patched OS CD)

# Prevention 103: Plan for recovery

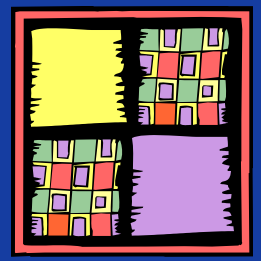
Other stuff to have in your recovery kit:

- A copy of your tape backup/restore software (if applicable).
- Your tape software license diskette or serial number needed for installation.
- A copy (printed or on floppy or on the ZIP drive!) of the most recent config.txt file.
- A checklist that works for you – especially at 3:00 AM with people yelling at you.
- Pack your kit-bag: Put it ALL in a box/bag so that you look in ONE place, find it all, and can carry it to another room or site immediately.



# Prevention 201: Patch that puppy!

- Novell doesn't issue new OS patches simply to torture us.
- Current support packs usually fix a lot more than they break
- It pays to keep current: if you're not patched to the current level of support pack, don't bother calling Support. Both Novell & Microsoft will tell you to apply the latest support pack and call back when you've reproduced the problem
- Edirectory needs patches, too! Go to: http://support.novell.com/filefinder/, and search for "ds.nlm"



# Prevention 202: Document & Maintain

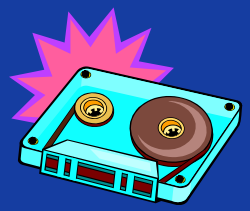
Investigate the wonders of the cron utility. Here are some tasks to consider automating:

- Run "**config.nlm /d**" automatically each night, prior to backup.
- Run "**dsrepair –rc**" on each server containing DS replicas each night, prior to your tape backup routine, to create backup dib sets. (This will make Novell DS Support very happy with you when you need to call them.)

- **Toolbox.nlm** is a terrific way to purge volumes after the backup runs … especially when the volume hosts print queues or applications that create and delete a million little stinkin' "lock" files. (Remember Paradox?)
- Chronic DS problems? Consider running unattended dsrepair operations each night.
- Document the heck out of the autoexec.ncf and startup.ncf files. (This is automatically inserted into your config.txt file.)

# Prevention 203:

## "Just back the darn thing up, willya!?"



- We don't care what the tape software vendors say, nothing beats "everything, every night."
- Many current applications use temporary "journal" files. Overlaying multiple incremental restore sets can honk up applications -- especially critical vertical market apps such as accounting, HR, practice management, etcetera.
- If you can't back everything up overnight, you need to figure out why.
- For most shops, the existence of cheap gigabit switches and NICs and large, fast tape drives means that unless you're running a very large disk array, you *should* be able to back up everything, every night.

# Prevention 203:

## "Just back the darn thing up, willya!?"

- Change the tapes out regularly.  One year's service, max. (They stretch, get dirty, and drop bits all over the floor!)
- Use a simple rotation that you can easily understand at 3 o'clock in the morning when you're trying to restore during an emergency.
- Cleaning tapes are good things. Listen to your tape drive.  Clean it when the little light flashes. You and your tape drive will both be happier with the result.

# Interlude: Roadside sights.

# Troubleshooting 101:

## So…what do you do when all heck breaks loose?

- Grab a blank pad of paper and pen … you're going to need it, both for yourself and in case you need to call Novell or Microsoft support.
- Keep a chronology. As you go through each of the below steps, note the current time (and date, if needed). It really will help you track the situation better.

# Troubleshooting 101:

## Determine the nature and scope of the situation.

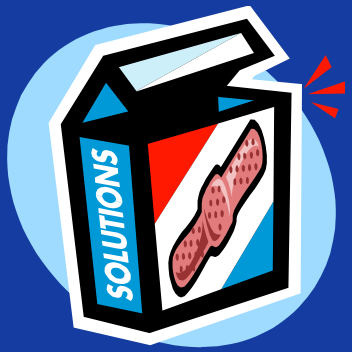
(Write all of this down on your blank pad, please)

- *What* are the symptoms?
- *Who* is affected by the problem?
  (Users, groups, buildings, campuses, etc.)
- *Which systems* are affected?
- *When* did this start? Today? Last night? Last week? (If the problem has been going on for a while, why is it just <u>now</u> being reported?)
- *What was changed* before the problem started?
- Politely inform people that this is NOT a time to "cover their tracks". Total truth is <u>essential</u> during network emergencies.

# Troubleshooting 101:

## Determine Possible Causes.

- Hardware (e.g., crashes)
- Software (e.g., ABENDs, BSODs)
- Infrastructure (network, power, WAN, internet, flooding)
- Configuration of any of the above items
- Operational/Procedural Error
  (our old friends “Fred” and “Simon”)



# Troubleshooting 101:

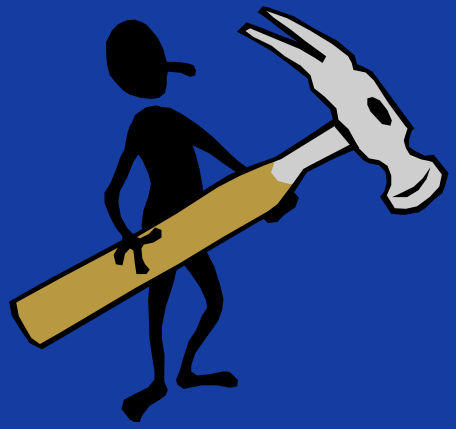
## Isolate the variables.

Hardware

- component swap
- firmware update
- configuration change

Software

- component update/upgrade
- driver upgrade
- configuration change



Procedural

- if you change the order of operations leading up to the problem, does it still happen?
- can you change the entry point?
  - Workstation(s) used
  - Login ID(s) used

# Troubleshooting 101:

## Start make changes … carefully.

WRITE IT DOWN - At each step, record what you've done, and what happened. It's far too easy to lose track of where you are if you don't write it down. (If you have a second person in the room, have them scribe for you while you're knee-deep in network blood and guts.)

CHANGE ONLY ONE VARIABLE at a time!

CHANGE EACH VARIABLE BACK to the original before trying a new variable. (There are exceptions, such as when changing a variable improves the problem.)

TEST THE SOLUTION - Using your notes of what the original problem was, try to replicate the problem

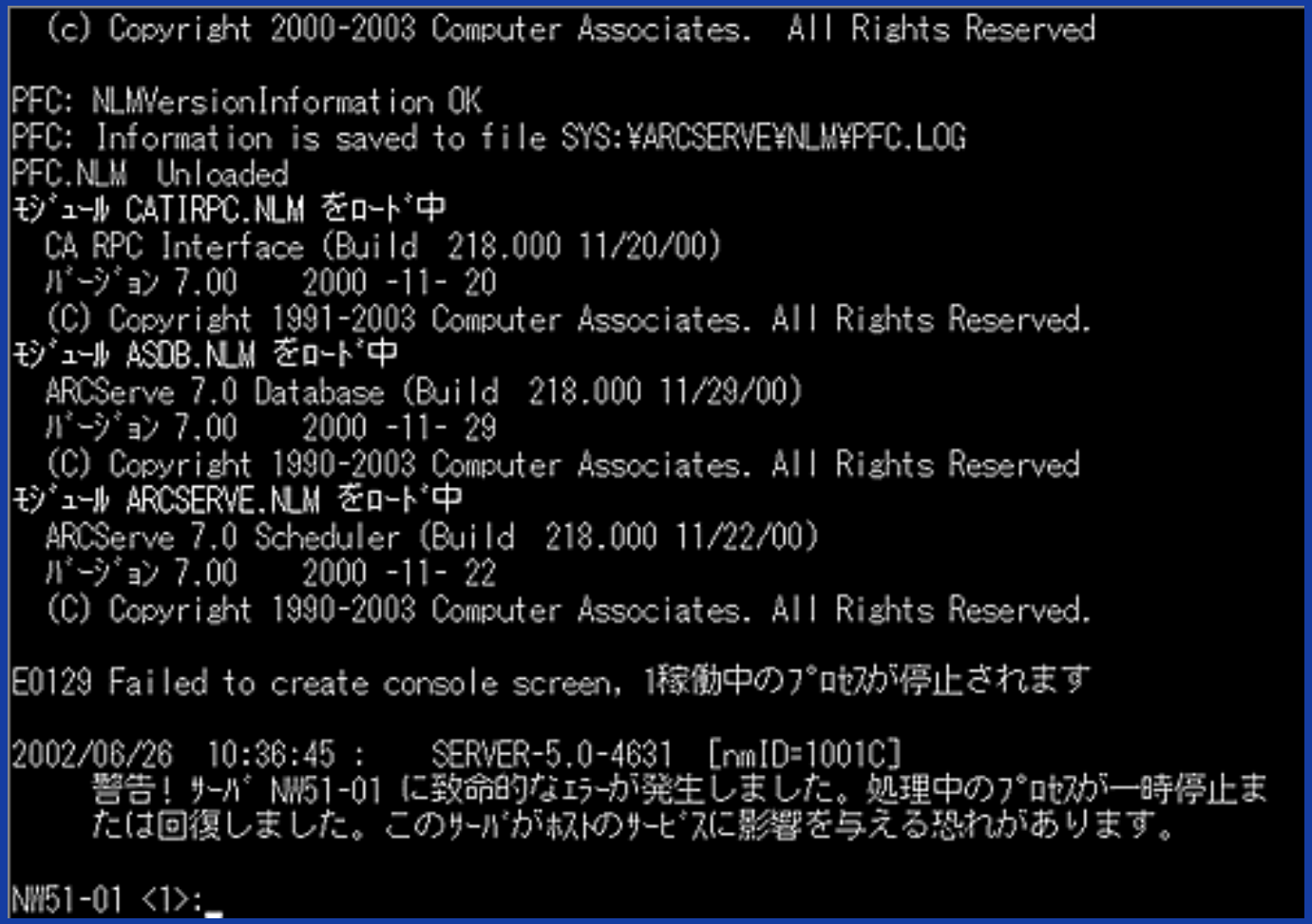
# Troubleshooting 102:

## When it's time to call Novell Support (1-800-858-4000) …

- Please have all of this information ready:
  - Support PIN …and password
  - OS version and patch level
  - DS version and patch level
  - List of third party products (version and patch level!) running
  - A copy of config.txt lists all vital server information … including system module dates and sizes.
  - A concise description of the problem
  - Your chronological notes…so support knows the exact sequence of events
  - A workstation, logged in as admin or equivalent
  - An abend.log file or an SPK Crash Report

- Remote access methods to consider (if needed):
  - PcAnywhere via dial-up or TCP/IP
  - Control-F1, Desktop Streaming, or similar web-based technologies

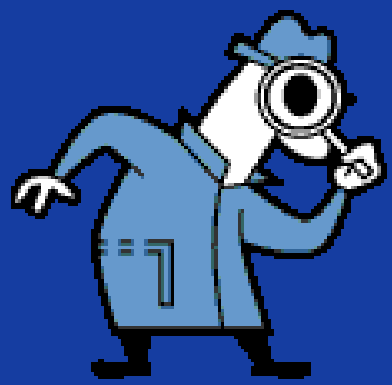
# Interlude: Abends Without Borders.



# Troubleshooting 200:

## "Welcome to the detective force!"

- These are the most difficult problems to resolve.
- Understand their nature: most ABEND and BSOD messages are programming "dead ends" for which the programmers didn't have time or energy to complete error routines.
- Your job is to figure out what's going on.



# Troubleshooting 201:

***"Everything should be made as simple as possible, but no simpler."* - Albert Einstein**

Solving a server crash is like solving a murder:

- Survey the crime scene
- Gather sufficient clues to resolve the cause
- Pinpoint your main suspect
- Identify secondary suspects

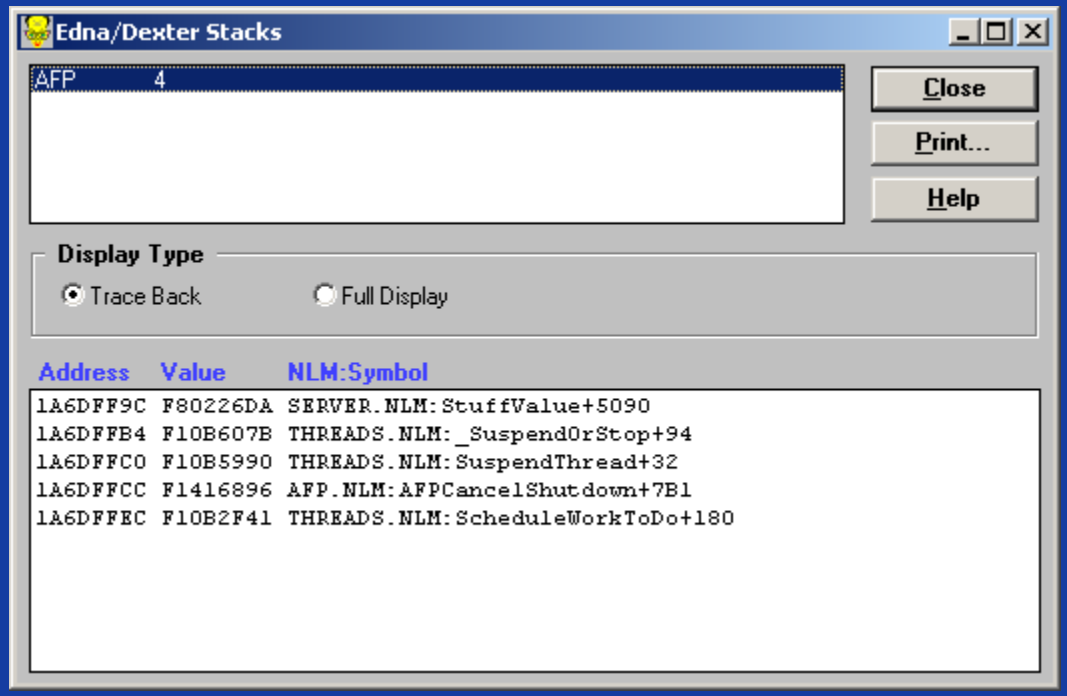
## Ask Three Questions:

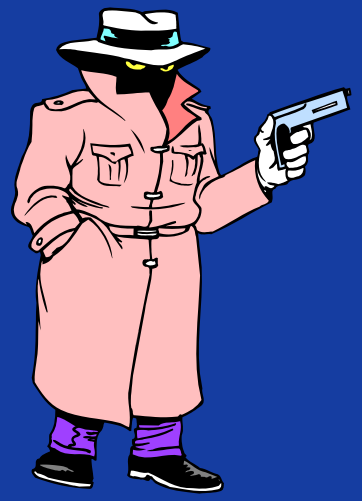
1. Which suspect (NLM/driver) pulled the trigger?
2. Did someone else force the suspect to pull the trigger?
3. Did someone else pull the trigger then put the smoking gun in the suspect's hand?

# Troubleshooting 201:

## Who was in the room when the gun was fired?

- The "room" is the program stack.
- The "who"s are the modules that were running.



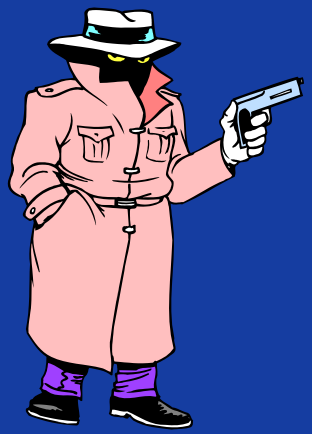



AdvisorEvents.com

# Troubleshooting 201:

## What usually causes problems?

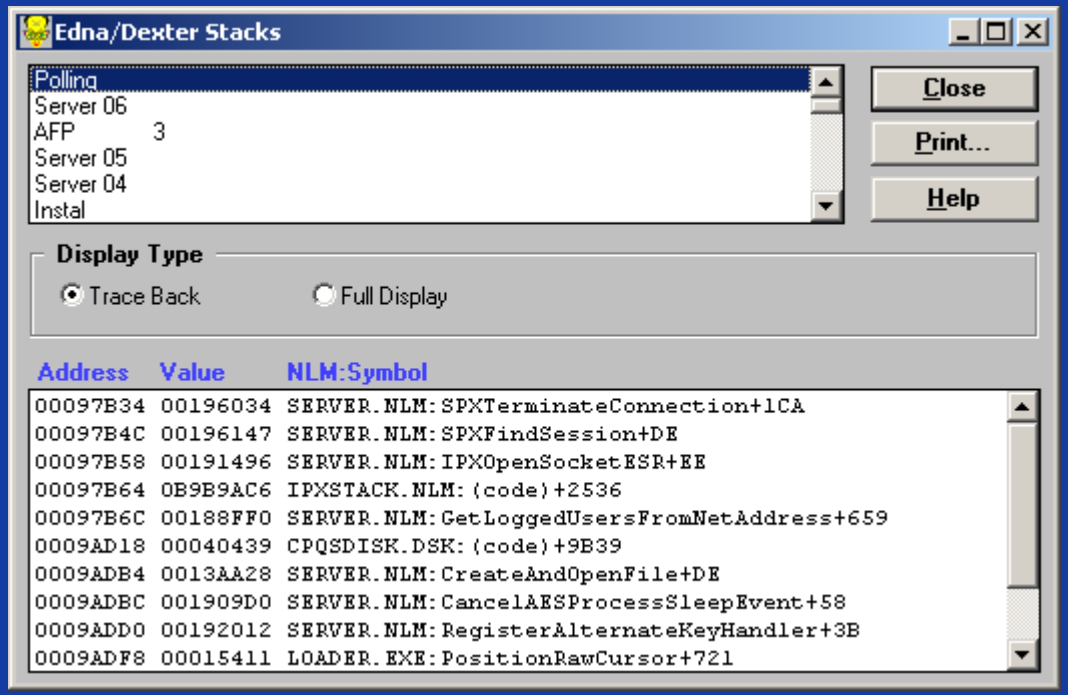
- Generally speaking … ignore the operating system (**NetWare™/Windows™/Linux/Unix**).
- It's the 3rd party stuff or other specific modules/drivers that usually bring the system down.



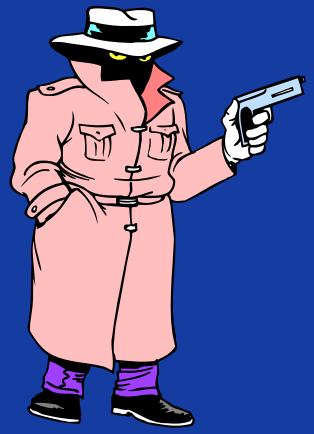
# Troubleshooting 201:

## Whodunnit?

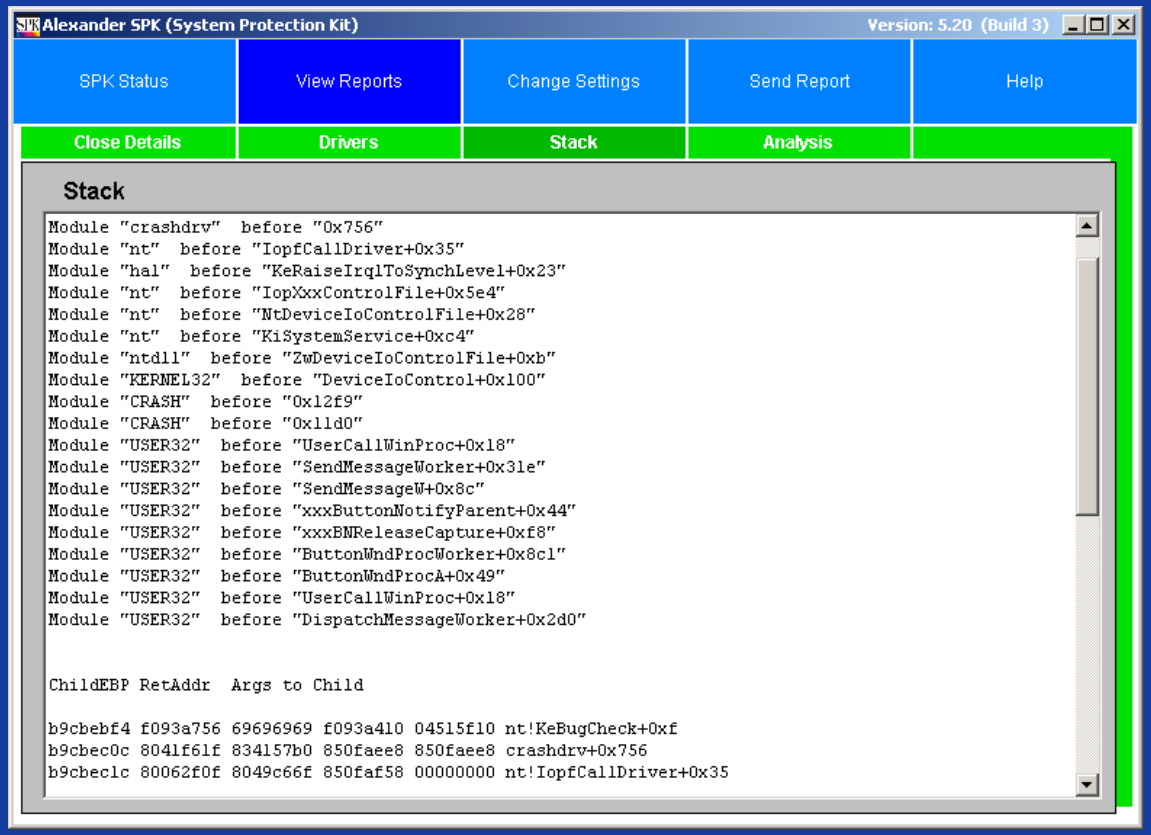
- So after you eliminate the core OS files, the modules you're left with are "who was in the room when the gun was fired"?



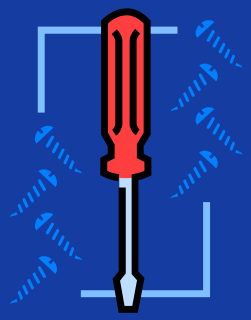

# Troubleshooting 201: Diagnosing ABENDs and BSODs



- The same thing goes for Windows:



# Tool Time:
# Let's review our tool box!

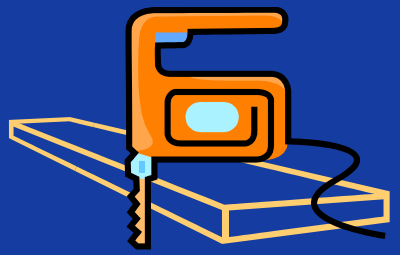


Config.nlm (DS) - (Loaded with NetWare OS.)

- Config.nlm creates a static file that isn't much help diagnosing a crash because it doesn't track system changes. However, it's critical for disaster recovery preparation.

Toolbox (AH) - (Loaded with NW51SP5 or NW6SP3 or later.)

- Allows you to purge deleted files and execute DOS-like commands and batch files at the server prompt.



Dsrepair (AH) (Loaded with NetWare OS.)

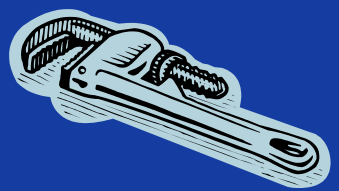
- This, or NDS iMon – learn it, live it, love it.

SPK (DS) – (Available at http://www.alexander.com)

- NetWare
- Windows

RecoverySafe (DS) – (Available at http://www.alexander.com)

- Windows Servers
- Windows PCs



AdvisorEvents.com

# Submit Your Stories & Topic Requests

We're gathering stories of woe and wonder from network admins, resellers, and consultants, for a series of articles for publication we're writing.

(We're also looking for article topic requests. )

Please let us know if you wish to remain anonymous or if it's OK to publish your name as a source.

Send your stories to:
stories@alexander.com



# Thank you!




Allan Hurst – allanh@kiscc.com
KIS Computer Center – http://www.kiscc.co



Resources:

- Novell Downloads – http://download.novell.com
- Novell File Finder - http://support.novell.com/servlet/filefinder
- Microsoft Symbols & Debugger: http://www.microsoft.com/ddk/debugging/default.asp


**Very special thanks** to the "Novell Oakland Bayarea User Group" (http://www.nobug.us) and to "Silicon Valley NUI" (http://www.nui.net/svnui) for their invaluable assistance in refining and testing this presentation.

**Support your local NUI chapter! (Find yours at http://www.nuinet.com)**