

HARDWARE, SOFTWARE, & NETWORK TROUBLESHOOTING

MacTech Boot Camp 2011
Chad Nielsen

INTRODUCTION

About Me (I'm Chad Nielsen, btw)



- Graduated in 2003, BA in Computer Science and Philosophy
- Worked for Apple Retail from 2004 to 2008 as a Genius
- Worked for Forget Computers from 2008 to present
 - Support Desk Manager and Casper Administrator

INTRODUCTION

About Forget Computers



- Managed Service Provider (MSP)
 - Team of 8 and Growing
- 80+ Clients across the US (mainly Chicagoland)
 - Manage Mac OS X 10.3 - 10.7

INTRODUCTION

About My Forget Computers Responsibilities



- Tier 3 support
- Casper Administrator

Application and OS Installation and Patching
Maintenance
Imaging Workflows
Security

- Knowledge Base and Checklists
- Change Management

INTRODUCTION

About This Talk



- Conditioning Your Mind to Troubleshoot
 - Largely Philosophical

The Questions to Ask
The Methods of Variable Elimination
The Tools

GOAL

a Troubleshooting Mindset that can be applied to any issue

INTRODUCTION

If You Get Bored



- Play Angry Birds
- Respond to Tech Support Emails from Family
 - Write Insightful Haikus
 - Sleep

I will not be offended!

INTRODUCTION

Outline

- The Troubleshooting Mindset
- Hardware Troubleshooting Scenario
- Software Troubleshooting Scenario
- Network Troubleshooting Scenario

TASTY Q&A - SHARE YOUR HAIKUS!

TROUBLESHOOTING MINDSET

What is it?

- Abductive Reasoning & Occam's Razor
- Mental Workflow to Ask the Right Questions
- Using the Information to Deduce Variables
- Intelligently and Efficiently Eliminate Variables

TROUBLESHOOTING MINDSET

Abductive Reasoning

Deduction

Allows derivation of b from a only where b is a formal consequence of a .

Deduction is the process of deriving the consequences of what is assumed.

Example

(**A**)

All humans are mortal.

(**B**)

The cast of Jersey Shore are humans.
(this is assumed for the sake of argument
and clearly debatable)

The cast of Jersey Shore is mortal.

Induction

Allows inferring b from a , where b does not follow necessarily from a .

We have good reason to believe the conclusion, but the truth of the conclusion is not guaranteed.

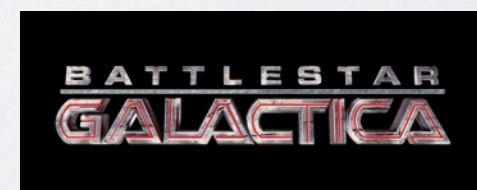
Example

(**A**)

All of the nerds I know like either Star Trek or Star Wars

(**B**)

Because I have no evidence otherwise It is reasonable to induce that **all** nerds like Star Wars or Star Trek.



TROUBLESHOOTING MINDSET

Abductive Reasoning

Abduction

Allows inferring a as an explanation of b .

Abduction provides possible explanations for determining the cause of the issue based on what we know.

Example

(**B**)

There is a quarter stuck in my optical drive.

(**B**)

My child was counting change on the kitchen table.

My child put the quarter into my optical drive.

TROUBLESHOOTING MINDSET

Occam's Razor

(it has, like, eleventy blades or something)



"The simplest explanation is often the right one."

NOT ABSOLUTE

HEURISTIC (LEARNING) DEVICE

Abductive Reasoning + Remembering Occam's Razor = **WIN**

TROUBLESHOOTING MINDSET

Before You Begin, Remember:

Do not rush.

It may take time.

The Subconscious.

You are a detective.

Be Methodical. PEBCAK.

Ego & Demeanor.

Use your intuition.

Let the user speak.

Speak at their level.

Confirm Urgency.

Their schedule.

MOMENT OF ZEN

clear your mind, prepare to troubleshoot



HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 1: Gather Information

What has changed?

workstation recently moved

no previous power issues in old location

no recent hardware upgrades

no unusual noises

Can you reproduce the issue?

intermittent

no pattern

no method of replication

Is the workstation the only device affected?

user has not noticed any other power issues with peripherals

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 2: List Possible Causes

Use your previous experience and information gathered.

power cable not plugged in

bad internal component

bad or unclean power source

workstation using outlet controlled by a light switch

user logging in through SSH and messing with user

bad battery inside of UPS

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

resseat the power cable (firm)

check the system.log for power errors (found)

check the service manual for error list (not found)

GOOGLE IT

GOOGLE TANGENT!

two minutes of biased honesty with Chad Nielsen

Google is the best tool in our arsenal.

Unmatched indexing of forums and support sites

Outstanding source of command line examples

Get a sense of the depth of your issue

To those who argue that using Google is
a weak form of troubleshooting:

SHUT THE FRONT DOOR!

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

reseat the power cable (firm)

check the system.log for power errors (found)

check the service manual for error list (not found)

Google It! (some mentions, no solution)

workstation plugged into outlet controlled by light switch (nope)

a user is logging in through SSH and turning off machine (remote login unchecked)

bad UPS battery (not beeping, shows condition normal)

APPLE HARDWARE TEST

APPLE SOFTWARE DIAGNOSTIC

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

APPLE HARDWARE TEST



quick test of memory and logic board

can do standard or extended testing (more memory checks)

comes with every Mac

APPLE SOFTWARE DIAGNOSTIC

EFI

low-level testing, runs in the firmware

not all components are tested

faster to load and run

OS

runs in Mac OS X

tests components that require OS drivers to activate

runs slower but overall better for stress testing a machine



HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

reseat the power cable (firm)

check the system.log for power errors (found)

check the service manual for error list (not found)

Google It! (some mentions, no solution)

workstation plugged into outlet controlled by light switch (nope)

a user is logging in through SSH and turning off machine (remote login unchecked)

bad UPS battery (not beeping, shows condition normal)

Apple Hardware Test (AHT)

Apple Software Diagnostic (ASD)

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 4: Component Isolation

you test the UPS instead of trusting it (the unit powers off!)

you notice that the peripherals are all plugged into the surge area

you try a new or known-good battery (no effect)

you try a new or known-good UPS (success!)

A fix, that's great! But why did the replacement work?



HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Step 5: Gather a Full Understanding

ASK QUESTIONS

Was the UPS faulty or damaged in the move?

What if the UPS was never moved, only the workstation?

INVESTIGATE AND CONFIRM

You speak with the user, they did not do the move but know which tech did.

You speak with the tech, they confirm they did not move the UPS from the original location.

You check the original UPS. It matches the one you used as a replacement.

The UPS in the original location was rated for a higher wattage!

When paired with the appropriate machines, both UPS units function normally.

CREATE / UPDATE CHECKLISTS AND PROCEDURES

HARDWARE TROUBLESHOOTING

scenario: a workstation is intermittently powering off

Overview

- 1. Gather information from the user.**
- 2. Determine what has changed.**
- 3. Determine if the issue can be reproduced.**
- 4. Determine the scope of the issue.**
- 5. Make a list of probable causes.**
- 6. Use abductive reasoning to eliminate each cause.**
- 7. Gather a full understanding to prevent / identify the cause in the future.**

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 1: Gather Information

What has changed?

user launches the app a few times a week

user says they did not update this app

user says they did not update other apps

Can you reproduce the issue?

intermittent

can sometimes be replicated

opening and saving files can trigger it

Is the workstation the only device affected?

this is the only workstation affected

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 2: List Possible Causes

Use your previous experience and information gathered.

application was updated without user's knowledge and was corrupted in the update

operating system was updated without user's knowledge, made it incompatible

application plist or support files are corrupt

application plist or support files have incorrect permissions

application uses a peripheral, network or local resource that it cannot find

bad RAM

bad CPU

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

kernel panic appears to be software related according to the log (TN2063)

confirm application and operating system updates were not performed

- check receipts
- check tripwire (compile from source, free)
- check the Casper Suite (installer, commercial)
- check creation dates
- check radmind (installer, free)
- check software update log

you confirm that no updates were applied

you log into Console and launch the app, locating an error that describes "bad access"

you search Console and find this error started around the same time as the kernel panics

you Google the error and check the forums - no information found

While you are investigating you notice the OS is very slow to respond.

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 3: Eliminate Possible Causes

we do not know which files to check

we cannot check each file

we do not know how to tell if a file is corrupt

It's time for a split / half search!

you create a new user, log in as that user, and the application works

the error is no longer in Console and you cannot replicate the kernel panic

you notice that the OS feels slow in the new user as well

Having narrowed the issue to the existing user, you decide to run a few tools to make sure there aren't any other problems on the disk.

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 3: Eliminate Possible Causes

Activity Monitor - CPU and RAM (both normal)

Disk Utility - Repair Permissions and Verify Disk

live verification in Disk Utility finds invalid sibling links it cannot repair

DIRECTORY REPAIR TOOLS

Single-User Mode (SUM): fsck and AppleJack

NetBoot or external hard disk with OS installed to run Disk Utility

Third-Party: Drive Genius, TechTool Pro, DiskWarrior

fsck is unable to repair the damage

you grab your copy of DiskWarrior and repair the damage

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 3: Eliminate Possible Causes

you test and replicate the issue in the existing user - the directory damage was unrelated

you check Console again - the same error persists

you decide it's time to use some tools to determine what files the app uses

Command Line: `fc_usage`, `lsOf`

Third-Party: `fseventer`

Try this on your Mac - it's neat!

1. Launch the app you wish to analyze.
2. Locate the PID using the command line: **`top`** or **`ps aux | grep <app name>`**
3. Start gathering info using `fc_usage` in command line: **`sudo fc_usage <PID>`**
4. Start using the app in the manner that causes the problem, watch for file paths!

you use `fc_usage` to find that the app is referencing a particular plist when loading / saving

You find that the plist is referencing a username that is not the username on the computer. You modify the plist to reflect the correct username, the Console error goes away and the kernel panics do not return.

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Step 4: Gather a Full Understanding

Kernel Panics

the username was changed

the app was coded so poorly it could not update its paths

deleting the plist may have also worked - but at what cost?

Directory Error

it's plausible that the directory error and kernel panics are related

forcing a machine to power off to restart can cause directory issues

you will never know this for certain, unless you had maintenance apps

installed prior to the problems (Casper Suite)

You speak to the user, and they admit that they were recently married and changed their last name. They used an app that was recommended to them to make the change and suspected they caused the error.

The user was too embarrassed to admit this in the information gathering phase.

SOFTWARE TROUBLESHOOTING

scenario: an application is causing a kernel panic on a workstation

Overview

- 1. Gather information from the user.**
- 2. Determine what has changed.**
- 3. Determine if the issue can be reproduced.**
- 4. Determine the scope of the issue.**
- 5. Make a list of probable causes.**
- 6. Use abductive reasoning to eliminate each cause.**
- 7. Gather a full understanding to prevent / identify the cause in the future.**

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 1: Gather Information

What has changed?

user noticed no new email had arrived

user attempted to use a web browser, could not connect

the workstation receives a valid DHCP address

Can you reproduce the issue?

the error is persistent

Is the workstation the only device affected?

this user is the only one reporting the issue

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 2: List Possible Causes

Use your previous experience and information gathered.

the DNS cache became corrupt and needs to be flushed

there are incorrect settings in the Network preference pane

there is a problem with the Ethernet port on the computer

there is a problem with the Ethernet cable

there is a problem with the Ethernet port on the wall

there is a problem with the switch

there is a problem with the router

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

you check the Network preference pane - no hard-coded entries

you renew the DHCP lease - no effect

you flush the DNS cache and restart the workstation - no effect

- Mac OS X 10.4: `lookupd -flushcache`
- Mac OS X 10.5+: `dscacheutil -flushcache`

you reseal the Ethernet plug going into the workstation and wall - no effect

you test with a known-good Ethernet cable - no effect

IT'S TIME TO USE TOOLS!

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 3: Eliminate Possible Causes

Use your previous experience and information gathered.

Command Line: host, dig, ping

Apple: Network Utility (lookup, ping, trace route)

Third-Party: WhatRoute (LAN, Address, Port scanner, free)

Examples

host <dns name> OR host <ip address>

dig <dns name> OR dig -x <ip address>

ping <dns name> OR ping <ip address>

If you notice any delays, use Network Utility > Trace Route or WhatRoute to determine where your slowdown is coming from.

You determine that there are no delays, that you have full access to the internal network and this workstation only goes to one router before it hits the outside world.

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 3: Eliminate Possible Causes

The Router - Troubleshoot or call an Expert?

the router is working for other users

making changes during the business day might take the router offline

For the sake of this talk, we shall proceed!

you should never power-cycle a router - it will lose unsaved modifications

you determine the make, model and login information for the router in question

you Google the manual and give it a quick read-through

you Google for similar problems and find that this exact error could occur if the router runs out of DHCP licenses!

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 3: Eliminate Possible Causes

you log into the router and using the manual you check the DHCP table
you find that you have 53 clients connected but you only have a license for 50
that means there are two more devices out there that no one reported
you do a device count and only find 38 devices
using what you've learned in the manual you save the router changes

you reload the router after hours and it resolves the issue!

the next day, the issue happens again but on a different workstation!

you know the quick-fix, but what is the cause of the DHCP table going beyond 50?

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Step 4: Gathering a Full Understanding

as you walk around the office you notice a large amount of people with personal music devices
one week ago Pandora and Last.fm were blocked to reduce network traffic

personal music devices - many of them have Wi-Fi!

the choice to block streaming music caused an entirely new network problem

You have two options:

1. You can increase the amount of DHCP licenses by upgrading the router.
2. You can prohibit employees from connecting their personal devices to the network.

you opt for upgrading the router

you understand the value of personal freedom in the workplace

the company is growing and an upgrade would have been needed in the near future anyway

NETWORK TROUBLESHOOTING

scenario: a user cannot connect to the internet on their workstation

Overview

- 1. Gather information from the user.**
- 2. Determine what has changed.**
- 3. Determine if the issue can be reproduced.**
- 4. Determine the scope of the issue.**
- 5. Make a list of probable causes.**
- 6. Use abductive reasoning to eliminate each cause.**
- 7. Gather a full understanding to prevent / identify the cause in the future.**

CONCLUSION

(please stop playing Angry Birds at this time)

Follow the steps in the overview.

If you reach an impasse, gather more information and start again.

Google is your best friend.

Consider posting on lists and forums for help.

Consult your colleagues before making changes.

TASTY Q&A

Overview

- 1. Gather information from the user.**
- 2. Determine what has changed.**
- 3. Determine if the issue can be reproduced.**
- 4. Determine the scope of the issue.**
- 5. Make a list of probable causes.**
- 6. Use abductive reasoning to eliminate each cause.**
- 7. Gather a full understanding to prevent / identify the cause in the future.**