Fun With Traces -- Beginner

http://www.skendric.com/seminar/

Stuart Kendrick
Sustaining Engineer
EMC Isilon

Grab a USB stick from up front if you want to perform your own analysis

The Concept

Fun With Traces

I developed this seminar as a day-long Hands-On Lab, in which we practice Wireshark techniques while analyzing real-world case studies.

Today, we have 75 minutes. Hmm. So, we'll shrink the solo practice time down to ~5 minutes per trace. And we may not reach all the traces. But I still predict fun!

I try to slip a lot of lessons into this format, from refining the Problem Statement to diagramming examples to leveraging your Problem Management process for communicating risk.

I promote interactivity: please interrupt, contribute, heckle as you see fit. Then again, if you prefer to sit back, watch, and listen, you are welcome to do that also.

I predict that you know ways to analyze these cases faster/better than I did … please share your techniques, and I'll demo them for all to see.

Mechanics

Talk

- I encourage interactivity
- If you want to contribute, feel free to interrupt me
- Or raise your hand, and I'll call on you
- I'm good with either approach

Traces

- Grab a USB stick from the table up front

This deck available at http://www.skendric.com/seminar/

Me

Multi-disciplinary IT trouble-shooter / Root Cause Analysis
http://www.skendric.com

sbk@cornella	*student*	*1981*
stuart@cpvax5 (Science Applications Inc)	*programmer*	*1984*
sbk@cornellc.cit.cornell.edu	*desktop / server*	*1985*
stuart.kendrick@med.cornell.edu	*server / network*	*1991*
skendric@fhcrc.org	*multidisciplinary*	*1993*
stuart.kendrick@ isi lon dot com	*sustaining engineer*	*2013*

IT Architect | ITIL Problem Manager | Problem Analyst | Device Monitoring | Transport

Geeky Highlights

PL/1 on IBM mainframes	*Cornell University*	*Ithaca*	*1981*
FORTRAN on CRAY-1	*SAIC*	*San Diego*	*1984*
Terak, DisplayWriter, IBM PC, Macintosh	*Cornell University*	*Ithaca*	*1985*
Netware, Corvus Omninet, TCP-IP / IPX / AppleTalk	*Cornell University*	*Ithaca*	*1988*
AppleShare, QuickMail, Farallon, NRC, Cisco, Sniffers	*Cornell Medical College*	*Manhattan*	*1991*
Solaris, Windows, Linux, Perl, SNMP, Wireshark, Cisco, Fluke	*FHCRC*	*Seattle*	*1993*
OneFS	*EMC Isilon*	*Seattle*	*2013*

Geek credentials: I missed punch-cards by one semester … grew up on shared machines (IBM and Cray) … my first network ran at 1Mb/s over Cat 2 (Corvus Omninet) carrying IPX + AppleTalk with IP encapsulated in both. I bored a vampire tap (once) … my first analyzer was a Network General Toshiba 286 laptop … and alpha versions of EtherPeek

Recruiting

I attend SharkFest for a lot of reasons …

But one of them is recruiting.

Isilon

If you would like to hear what it is like to work at Isilon, I would enjoy sharing the pros, and the cons, of working in this space.

You may not be interested in changing jobs right now – from my point of view, I would still enjoy talking with you – perhaps your situation will change in a year or two. *Isilon invests long-term in staff; a multi-year courtship suits our style just fine.*

Richly complex product, engineering-oriented company, plenty of difficult problems to solve.

Global company, numerous locations, and once you're sufficiently senior, plenty of flexibility in terms of operating remotely, telecommuting, and visiting a base office every quarter or so.

FHCRC

My old position at the Hutch is still open … Problem Manager / Problem Analyst, with oversight over Change Management and post-mortems arising from Incidents.

Come find me during a break or in the evening. Professional networking is a good thing.

Customer
Customer Facing
Internal Mostly
Meta-Information

The World According to Post-Release Engineering

An explicitly self-centered view of Isilon, an EMC business unit
~1400 world-wide / ~700 Seattle
~ $1 billion sales

Find Bugs

Customer

Historically, dominated by media, entertainment, and genome sequencing. Today, expanding into chip design, financial sector, home directories, medical imaging, oil & gas exploration, surveillance.

Account Management

District Account Managers
Sales Account Managers
Sales Engineers

Owns relationship with the customer

Escalation Management

Escalation Managers
Customer Service Managers

Coordinate response to critical customer issues

Host daily Critical Accounts & Customers (CAC) conference calls

Desktop, AV, Network
IT Field Client Services

Documentation
InfoDev

Field Services

Customer Engineers - EMC/Unisys
Hardware replacement
Boots-on-the-ground

Field Service Specialists - EMC
On-site trouble-shooting
Upgrade support

Fly & Fix Engineers
Proof-of-Concept Support
On-site recovery

Technical Account Managers
Proactive Technical Support
Problem Management
Service Management

Support

Remote Reactive Support

Dedicated Service Engineers
Customer-specific

Technical Support Engineers Levels 1 - 2
Service Request Owners
Heavy-lifting tech support

Geography

Bangalore, India	USA
Cork, Ireland	Durham, NC
Shanghai, PRC	Hopkinton, MA
Tokyo, Japan	Plymouth, MN
	Santa Clara, CA
	Draper, UT
	Seattle, WA

Validate Bugs

Recovery Team
Code Red intervention

Technical Support Engineers Levels 3 - 5
Coaches and Subject Matter Experts

Global Services

Professional Services
Migrations & Consulting

Serviceability
Process Improvement

Readiness
Gatekeepers for releasing patches, MRs, hardware

Executive Office

CEO
COO
CTO
Product Vision
Marketing
Product Mgmt
New Features

Engineering

Post-Release Engineering

Patches & Maintenance Releases

PRE CSE
Customer <=> Engineering link

Sustaining Engineering — *Triage Escalations*

PRE Dev — *Fix Bugs*

Fix Bugs

PRE Test — *Test Fixes*

Tools + Processes

Values

Customer first
Create the future
Be your best, expect the best
Execute
Have fun

Program Management
Lab Management

Core Engineering

Design & Build the next major release

Data Services
Control Path
HDFS
Job Engine
SmartLock
SyncIQ
User Interfaces
...

File Systems
Infrastructure
Data Path
Locking
RBM
Features
De-dupe
SmartPools
Snapshots

Platform
BSD
Group Management
NFS
...

Hardware

Fix Big Bugs

Create Bugs

Performance
Make it go faster

Protocols
AIMA
LIkewise
SMB

Virtualization
CloudPools
NDMP

Certification
Find bugs before shipping
QA
Longevitiy testing
Test Automation

Stuart Kendrick 2014-06-11

Case Studies

Case 1	Many Applications Crash	BlueHeat
Case 2	VMWare Cannot Mount SAN	The Router is Broken
Case 3	HL7 Transfers Interrupted	eGate Eccentricity
Case 4	Compile Host Aborts	Mainframes are Weird
Case 5	The Network is Slow	We Need a Bigger Boat

Case 1
Many Applications Crash

BlueHeat

Case 1: Background

This is the last week in November 2005. Earlier this year, we bought a mass storage device – a BlueArc Titan NAS head named *Indigo* sitting in front of 14 TB of Fibre Channel, SATA, and ATA attached disk trays. We have been migrating home + shared directories for two divisions (~1200 staff) from a flock of aging DAS-equipped file servers onto *Indigo*, along with scratch space for the MIS group.

The experience has been rocky. Starting in June, an OS memory leak caused key processes to hang and sometimes even head freezes, both requiring reboots to fix. A controller fried, requiring emergency downtime for replacement. A controller firmware bug mangled a volume, leading to data loss. We have been applying hot fixes, firmware upgrades, and OS upgrades every few weeks. Starting in August, users began reporting crashing applications – notably Outlook, although Word and Excel and other applications hang as well, intermittently – some days are fine, some days are bad. The MIS group's Tidal jobs fail regularly.

Backups are slow and sometimes don't complete – we aren't meeting our 24 hour Recovery Point Objective, and we have no confidence that we can meet our 48 hour Recovery Time Objective. *Sometimes even simple file copies are slow!*

Case 1: More Background

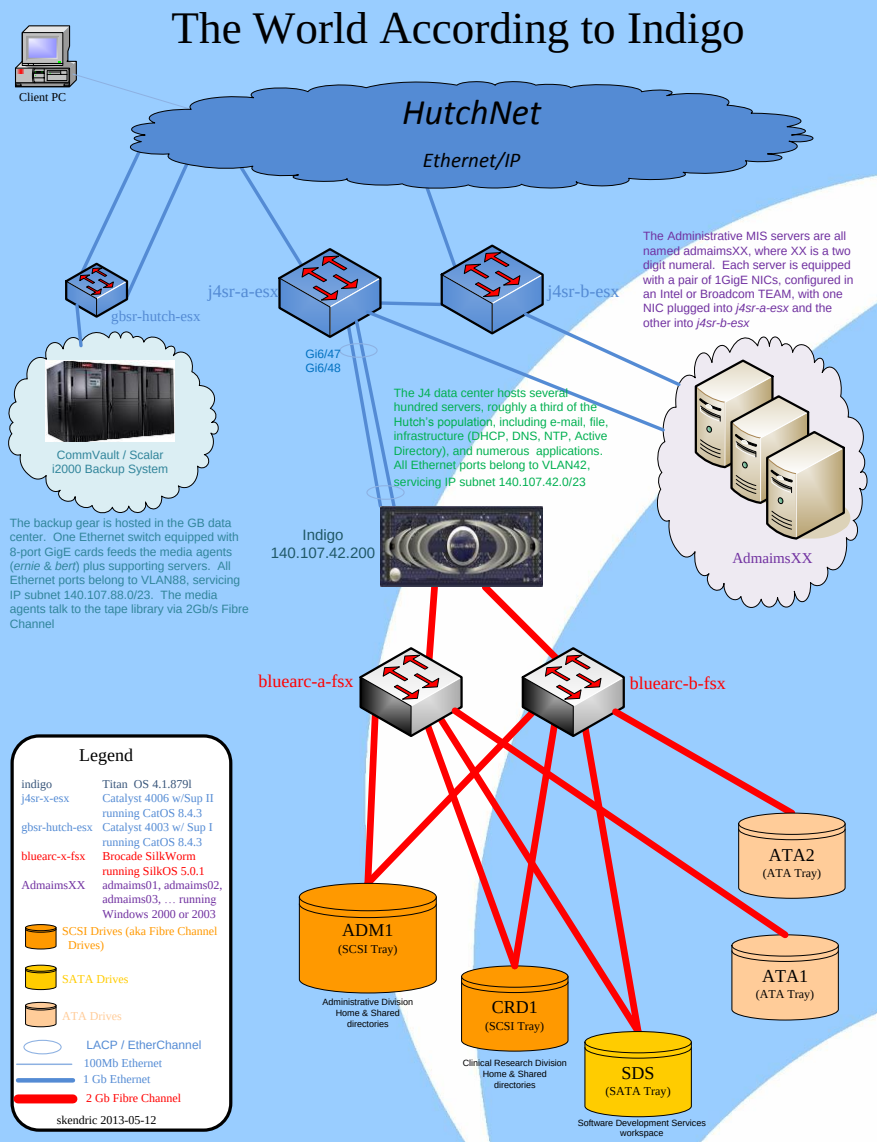
The storage team was convinced that antivirus scanning was causing the application crashes and has worked with BlueArc for months to resolve this, finally disabling AV over Thanksgiving. However, the intermittent application crashes continued this week.

The local BlueArc team visited a few days ago and identified the Catalyst 4000 Ethernet switches as the likely culprits: *"The Catalyst 4003 servicing the backup systems dates to 1998; the Catalyst 4006 servicing the Titan itself dates to 2000 – they are getting overwhelmed by traffic."*

The remaining ~1500 users who have not migrated to *Indigo* are watching with dismay – currently, they are unaffected, scattered as they are between small NetApp NAS heads and a flock of aging file servers.

Management has made every Sunday night in December available to you for *Indigo* downtime – just ask.

Case 1: Many Applications Crash



Case 1: Problem Statement

Initial Problem Statement

The switch is overloaded and is dropping packets.

Improved Problem Statement

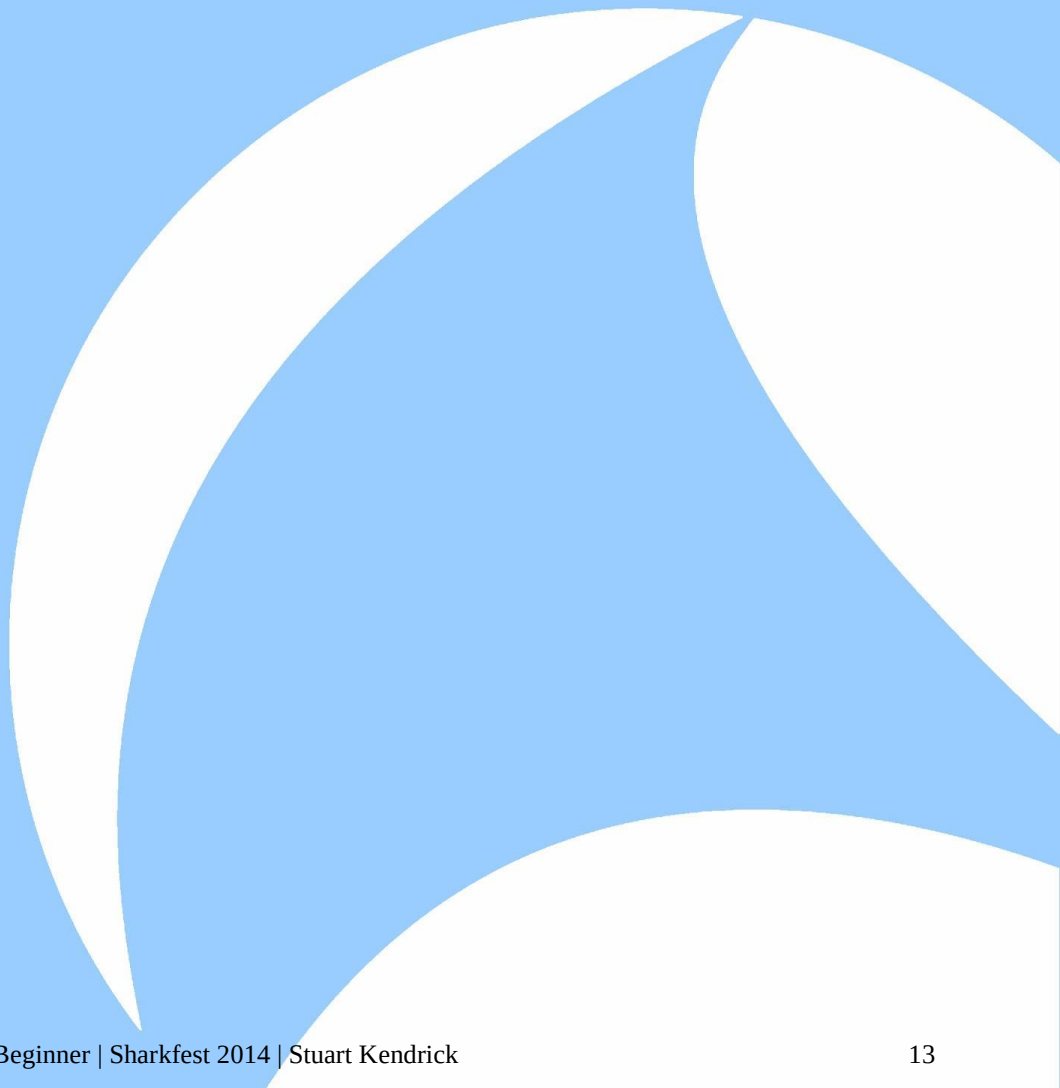
File copies are intermittently slow.

Buff it up a little more

Normally, a 10MB file copies in less than two seconds; but sometimes, the same file requires a minute or more to copy.

Case 1: Tell the Story

Who will recap for us?



Case 2
VMWare Cannot Reach Storage

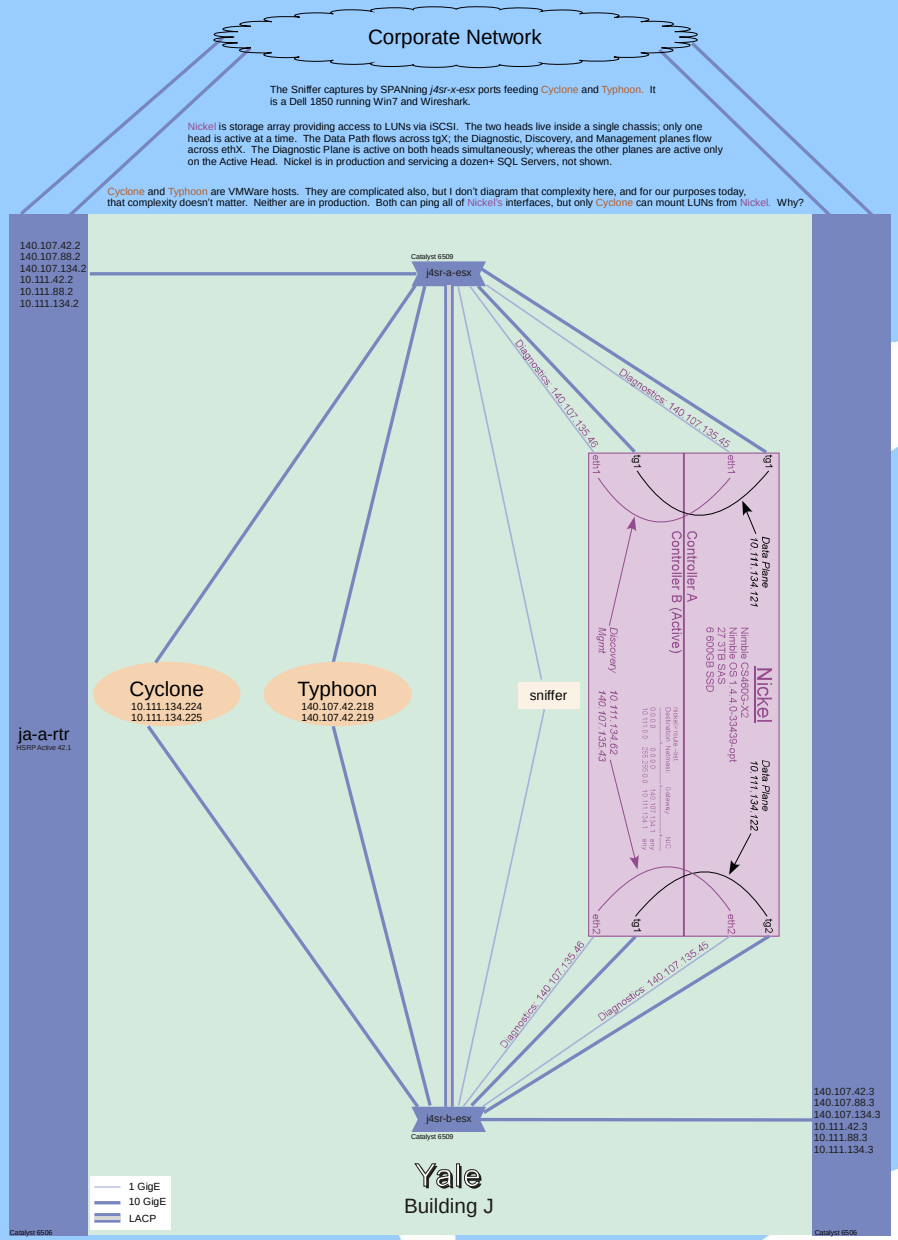
The Router is Broken

Case 2: Background

The storage folks have brought up their spiffy new SAN, a Nimble iSCSI box called *Nickel*. They are taking a gamble with it – Nimble was a new manufacturer at the time, just a few years old. During the eval and Proof of Concept phases, they found all sorts of immaturity. Still, the price was right, so they went with it. The box was intended to service both our VMWare farm (~1000 VMs distributed across 7 hosts) and a dozen SQL Servers (running PeopleSoft).

The VMWare farm moved first, and the results were spectacularly good (well, the previous SAN was overloaded, so just about anything would look good). But the SQL Servers had a different experience – the dev boxes did fine, but when production arrived, problems soared (performance and SQL crashes). After months of wide-spread disruption and slowness, the storage admins fixed a misconfiguration on *Nickel*, loaded a patch for a particular bug from Nimble, and life improved substantially.

The VMWare folks want to upgrade from VMWare 4 to VMWare 5 and refresh hardware as well. They have heated up two new boxes, *Cyclone* and *Typhoon*. *Cyclone* can mount LUNs off *Nickel* just fine, but *Typhoon* cannot. VMWare offers no error message – but the configured LUNs remain greyed out in the GUI. VMWare and Nimble tech support say everything is fine from their point of view and suggest that the router is broken, because *Cyclone* shares the same subnet as *Nickel*, but *Typhoon* is on a different subnet. Pings get through just fine and other hosts located in this data center and in other data centers mount iSCSI LUNs off *Nickel* *(and other SANs)* through this router just fine.



J4 Data Center
120 KW
~600 active MAC addresses
~1200 active IP addressees

HSRP
ja-x-rtr are HSRP Partners
Hello 3, Timeout 1
Generally, *ja-a-rtr* is HSRP Active and thus owns 140.107.42.1, 140.107.88.1, 140.107.134.1 ...

VLANs
All Ports on *j4sr-x-esx* belong to the same VLAN: VLAN42
The VLAN42 interfaces on *ja-x-rtr* support secondary IP addressing
140.107.42.0/23
140.107.88.0/23
140.107.134.0/23
10.111.42.0/23
10.111.88.0/23
10.111.134.0/23

skendric 2014-04-26

Case 2: Problem Statement

Initial Problem Statement

The router is blocking iSCSI

Improved Problem Statement

Typhoon cannot mount iSCSI LUNs from *Nickel*

Can you think of a better Problem Statement?

Case 2: Traces

A network admin and a VMWare admin collaborate

They first SPAN the *j4sr-x-esx* ports feeding *Cyclone* and capture a successful LUN mount into two trace files (they configure Wireshark to write two traces files – they don't know about Wireshark's ability to capture on multiple interfaces and write the results to a single trace file.)

And they repeat the process with *Typhoon*, capturing a failed LUN mount

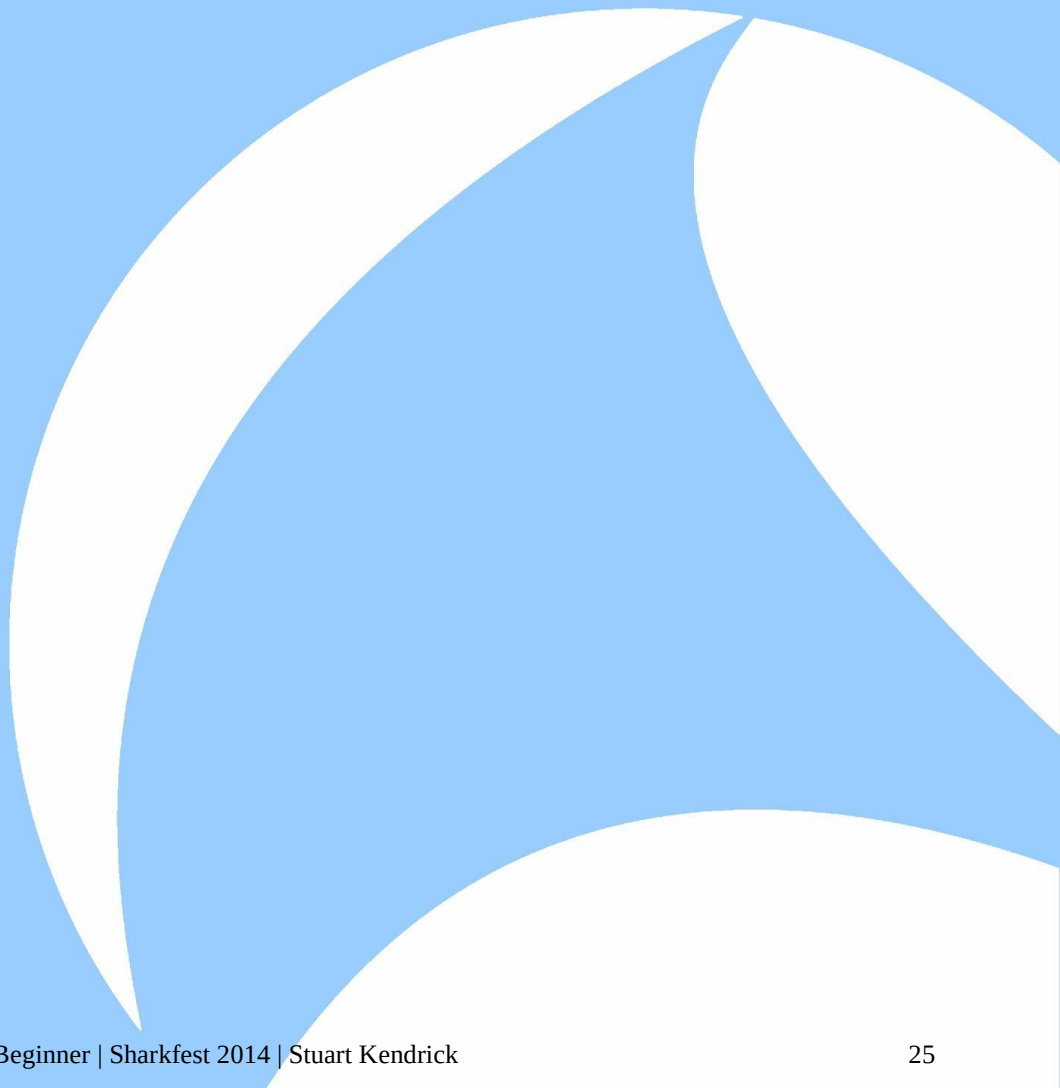
Cyclone-Capture-on-j4sr-a-esx-Port merged with Cyclone-Capture-on-j4sr-b-esx-Port =
Cyclone-Both-Ports-Merged

Typhoon-Capture-on-j4sr-a-esx-Port merged with Typhoon-Capture-on-j4sr-b-esx-Port =
Typhoon-Both-Ports-Merged

[BTW: *Cyclone* and *Typhoon* are actually the same box, with IP addresses reconfigured. For our purposes today, this detail does not matter.]

Case 2: Your Story

How would you tell this story?



Case 3
HL7 Transfers Interrupted

eGate Eccentricity

Case 3: Background

Two servers, *Minnie* and *Simba*, exchange updates every hour, keeping each other apprised of changes made by their respective user bases. They each run *eGate*, an application gateway which specializes in exchanging Admit / Discharge / Transfer (ADT) information between medical IT systems, often between hospitals, allowing each side to transform the incoming data in ways which suit its internal systems. It speaks the HL7 protocol, a popular protocol for over-the-network data exchanges amongst healthcare systems.

These data exchanges sometimes fail. When that happens, a monitoring process sends e-mail to the on-call DataBase Admin, who can intervene to retry the transfer.

Historically, the DBA has ignored the message, relying on the next hourly data transfer event to succeed (this reliably executes both current updates and previously failed updates, i.e. no data is lost). However, the team is becoming concerned, as the frequency has been gradually increasing – last year, the frequency was once every few weeks; more recently, several times a day.

There are times when the user base would rather not wait two or more hours to see the latest data. Management has heard their concern, and now the on-call DBA must respond to the alarms, 7x24x365. Sometimes, this is happening several times a night.

Case 3: More Background

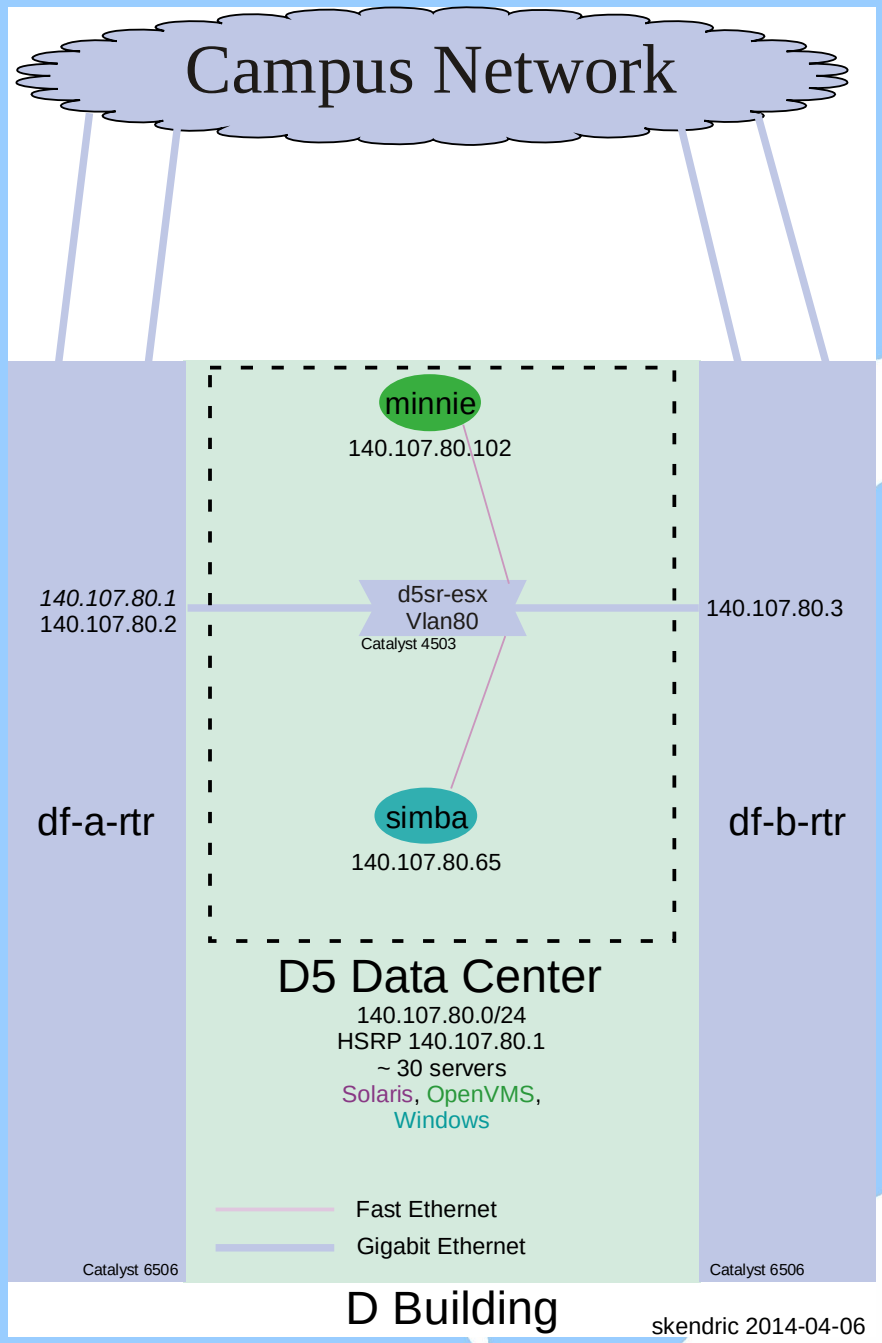
Management is concerned about the sleepless DBA issue; but they want you working on bigger problems and so ask you to ignore this.

You're sympathetic to your DBA buds – getting woken up each night is no fun.

One of the DBAs installed Ethereal on Simba years ago.

So, you show Mike how to set up a rolling capture; he understands how important it is to record event times precisely; and you tell that you'll spend an hour max analyzing whatever he finds.

A few days later, you get a handful of traces plus time estimates on when the transfer failed.


Campus Network
minnie
140.107.80.102
140.107.80.1
140.107.80.2
d5sr-esx
Vlan80
Catalyst 4503
140.107.80.3
df-a-rtr
simba
140.107.80.65
df-b-rtr
D5 Data Center
140.107.80.0/24
HSRP 140.107.80.1
~ 30 servers
Solaris, OpenVMS,
Windows
Fast Ethernet
Gigabit Ethernet
Catalyst 6506
Catalyst 6506
D Building
skendric 2014-04-06

Case 3: Problem Statement

Initial Problem Statement

eGate transfers intermittently fail with ‘A Network Error has occurred’

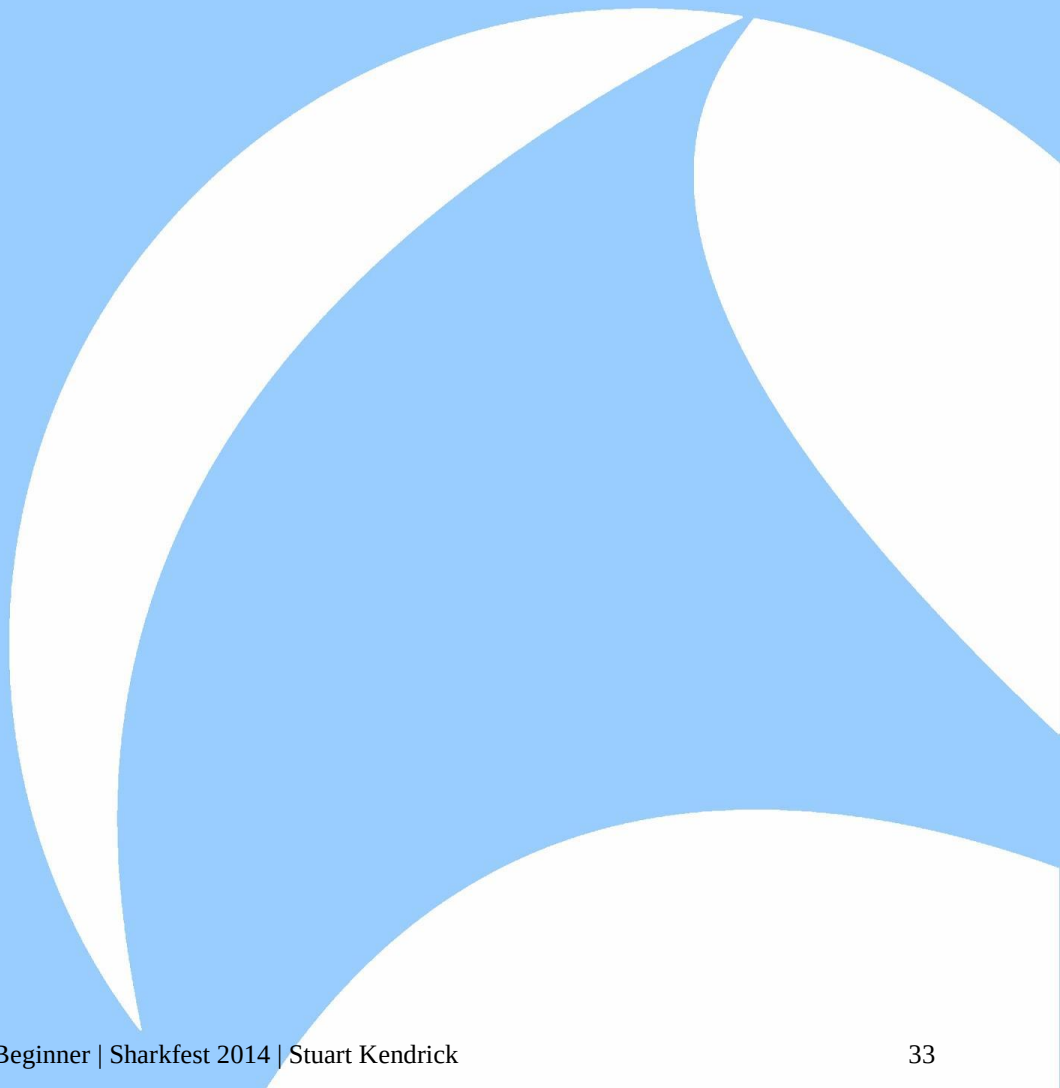
Let’s look at one of them: *eGate-Fail-2011-04-17-0607.pcapng*

Xfer failed somewhere around 20:56

Filter on tcp.stream==0

Case 3: Tell the Story

How would you tell the story?



Case 4
Compile Host Crashes

Mainframes Are Weird

Case 4: Background

The dev team compiles their software using IBM mainframes running z/OS, hosting the source files on a NAS Box, communicating via NFSv3. This workflow has worked fine for years when hosted on Manufacturer X, worked fine during the multi-month Proof-of-Concept using Manufacturer Y, but now that they are migrating production onto NAS Box Y, the compiles intermittently abort. A typical compile run takes days, these compiles are aborting at various stages during that process, never at the same point. They tend to crash early in the runs, after mere minutes

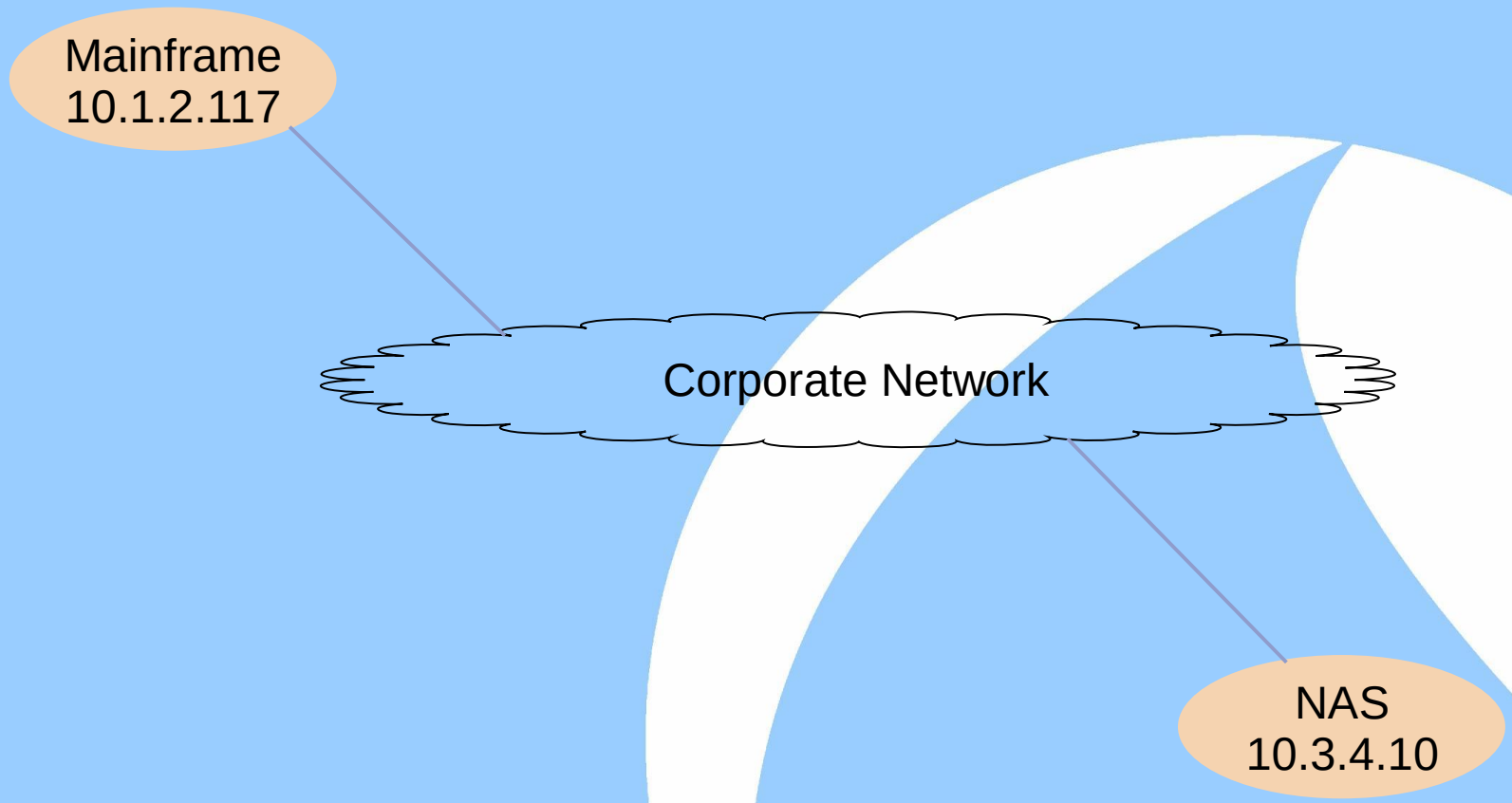
Their compile environment is richly complex and makes heavy use of both soft and hard links, which are traditionally difficult for NFS clients to handle properly:

http://plan9.bell-labs.com/sys/doc/lexnames.html

They have developed a test scenario in which the crash occurs after just a few seconds into the run and have captured the result using *tcpdump* on the NAS box

NAS Manufacturer Y has a strong reputation for being able to handle streaming NFS workflows at high-performance

This isn't much to go on. However, looking at the trace, can you offer any insights?


Mainframe
10.1.2.117
Corporate Network
NAS
10.3.4.10

Case 4: Problem Statement

Initial Problem Statement

Mainframes are weird

Improved Problem Statement

Compile jobs intermittently abort

Can you think of a better Problem Statement?

Case 4: Trace

If the operator lets the capture continue, you'll see the Mainframe pause for ~150 seconds and then send a TCP RST to the NAS Box (not shown in this trace).

Case 4: Your Story

How would you tell this story?

There isn't much to go on here – but can you rule anything out?

Case 5
The Network is Slow

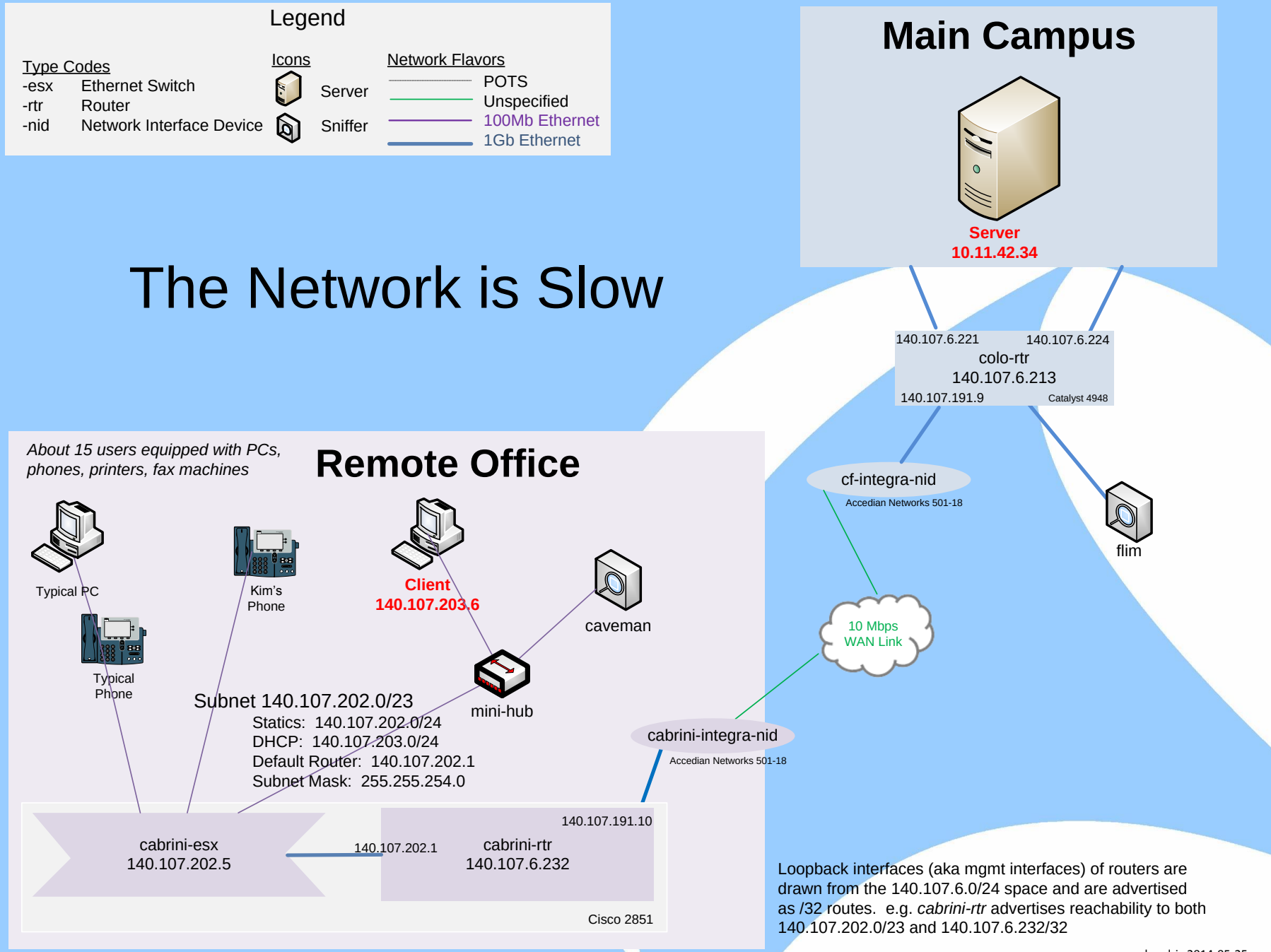
We Need a Bigger Boat

Case 5: Background

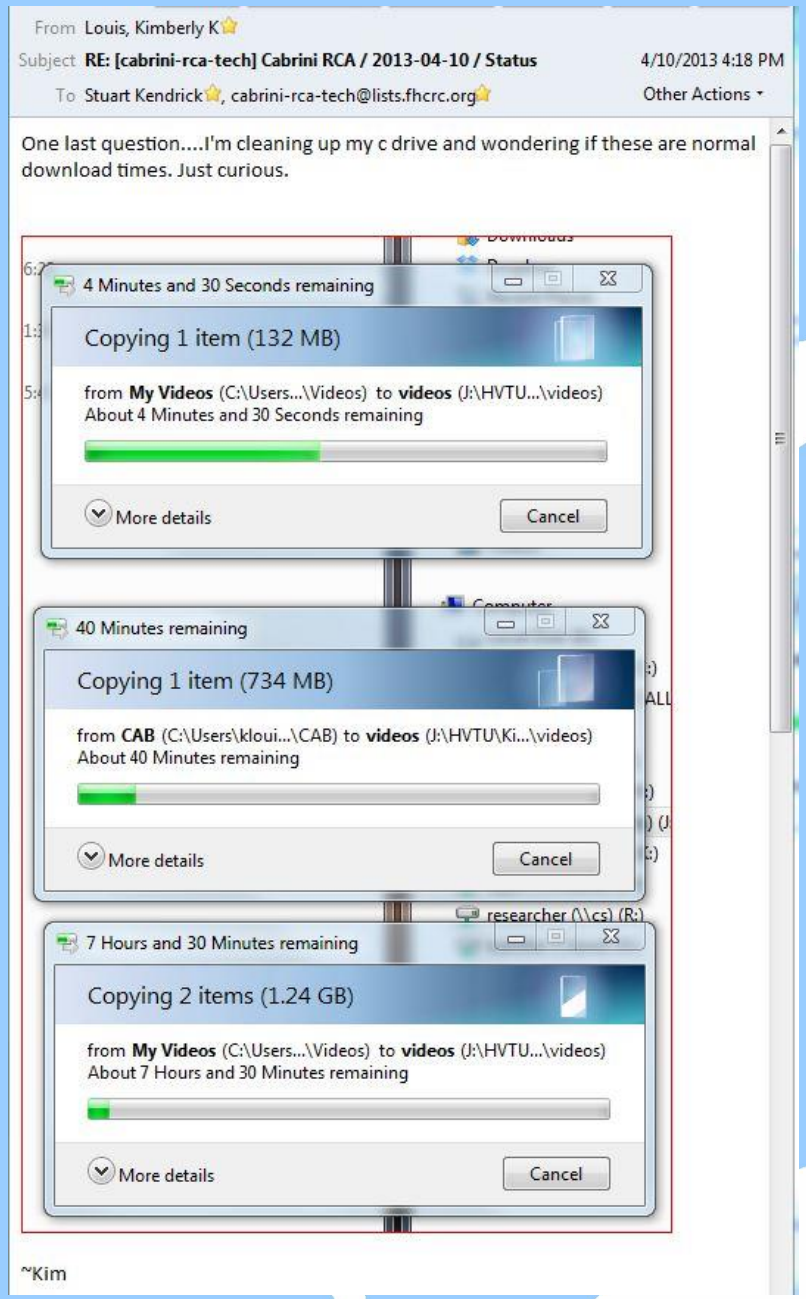
A remote office links back to the main campus via a 10MB/s Transparent LAN Service (TLS), a distance of several miles as the crow flies. Users complain of poor performance and want a bigger WAN pipe – they suggest that 100MB/s sounds like the next step

The current monthly cost is straining the budget, jumping to 100Mb/s would double or triple the cost and require signing a long-term contract … management wants evidence that taking this step will improve the end-user experience

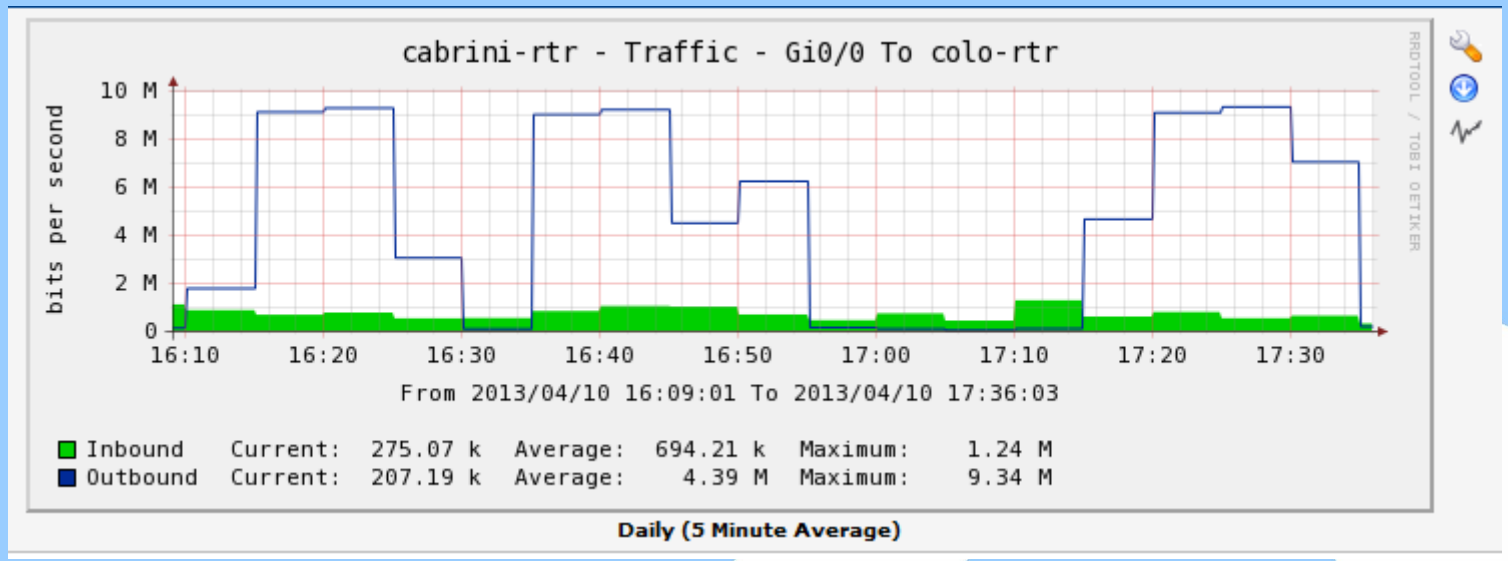
You are asked to estimate the effect on the end-user experience, were the TLS to be upgraded


Legend
Type Codes
-esx Ethernet Switch
-rtr Router
-nid Network Interface Device
Icons
Server
Sniffer
Network Flavors
POTS
Unspecified
100Mb Ethernet
1Gb Ethernet
Main Campus
Server
10.11.42.34
The Network is Slow
140.107.6.221
140.107.6.224
colo-rtr
140.107.6.213
140.107.191.9
Catalyst 4948
cf-integra-nid
Accedian Networks 501-18
flim
10 Mbps
WAN Link
cabrini-integra-nid
Accedian Networks 501-18
About 15 users equipped with PCs, phones, printers, fax machines
Remote Office
Typical PC
Typical Phone
Kim's Phone
Client
140.107.203.6
caveman
mini-hub
Subnet 140.107.202.0/23
Statics: 140.107.202.0/24
DHCP: 140.107.203.0/24
Default Router: 140.107.202.1
Subnet Mask: 255.255.254.0
cabrini-esx
140.107.202.5
140.107.202.1
140.107.191.10
cabrini-rtr
140.107.6.232
Cisco 2851
Loopback interfaces (aka mgmt interfaces) of routers are drawn from the 140.107.6.0/24 space and are advertised as /32 routes. e.g. cabrini-rtr advertises reachability to both 140.107.202.0/23 and 140.107.6.232/32
skendric 2014-05-25

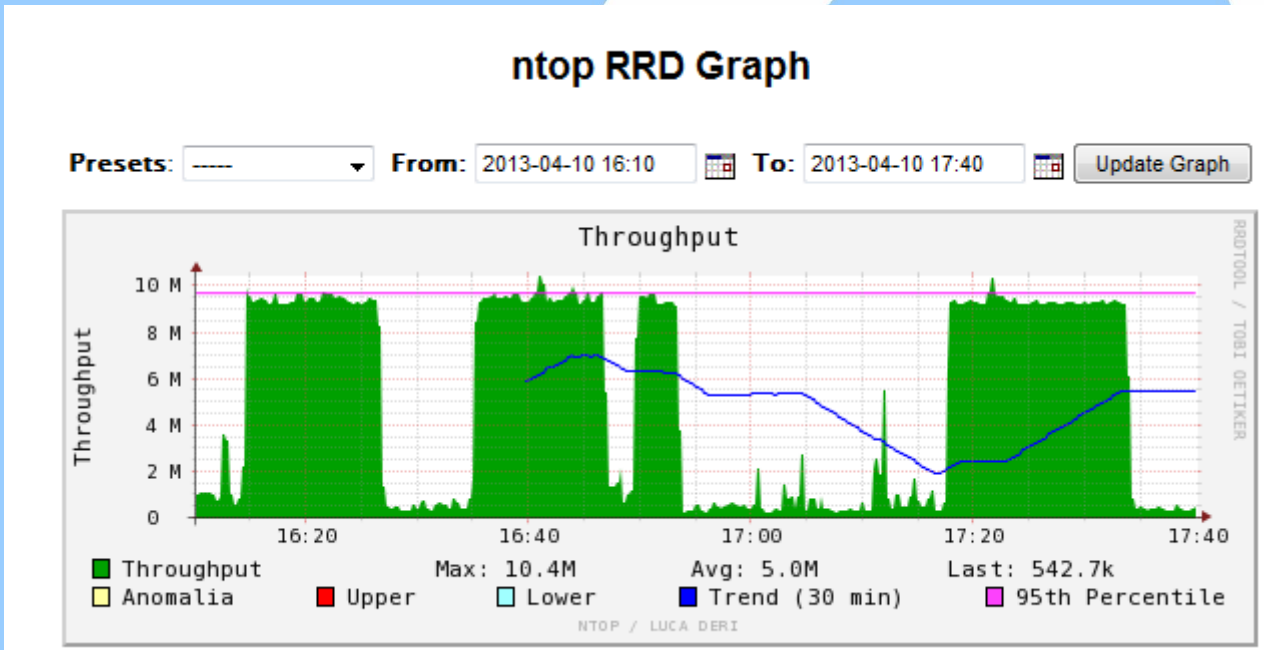
Kim is a power user who works on big documents locally, then copies them to her home drive on a server at the main campus nightly, to make sure they get backed up



Cacti


cabrini-rtr - Traffic - Gi0/0 To colo-rtr
bits per second
10 M
8 M
6 M
4 M
2 M
0
16:10
16:20
16:30
16:40
16:50
17:00
17:10
17:20
17:30
From 2013/04/10 16:09:01 To 2013/04/10 17:36:03
Inbound Current: 275.07 k Average: 694.21 k Maximum: 1.24 M
Outbound Current: 207.19 k Average: 4.39 M Maximum: 9.34 M
Daily (5 Minute Average)
RRDTOOL / TOBI OETIKER

nTop


ntop RRD Graph
Presets: -----
From: 2013-04-10 16:10
To: 2013-04-10 17:40
Update Graph
Throughput
Throughput
10 M
8 M
6 M
4 M
2 M
0
16:20
16:40
17:00
17:20
17:40
Throughput Max: 10.4M Avg: 5.0M Last: 542.7k
Anomalia
Upper
Lower
Trend (30 min)
95th Percentile
NTOP / LUCA DERI
RRDTOOL / TOBI OETIKER

Case 5: Problem Statement

For the purposes of this task, we're not analyzing a problem – we're not trying to figure out why end-users experience slow performance for example – so I don't have a classic Problem Statement to offer

Instead, we're attempting to perform an *Application Assessment* – given a hypothetical change in the environment, how would a given application behave? Colloquially, I call this *Predicting the Future* … in my experience, a generally fruitless endeavour

Prediction is very difficult, especially if it's about the future – Niels Bohr
Predicting is hard, particularly the future – Yogi Berra

Nevertheless, no need to throw our hands up in despair and run away. Instead, we can at least gather clues which management can use to inform this decision

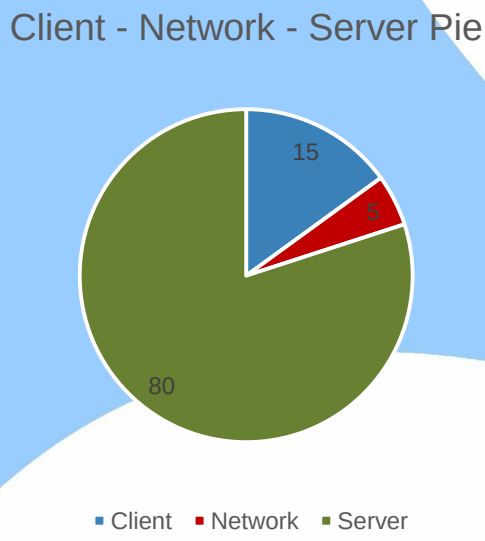
Ideally, we would tackle this task from various angles, typically using simulation for each of the applications in use. For our purposes today, we'll pick one application (file copy) and use packet traces to draw the Client-Network-Server Pie. Is this the best way to inform management's choice? No, but this is a class about trace analysis, so here we go

Case 5: Traces

We have two traces, one taken from the remote office (the sniffer *Caveman* plugged into a mini-hub shared by a user's workstation), the other taken from the main campus (the sniffer *Flim* plugged into a SPAN port on the switch at the main campus end of the TLS)

Effectively, for our purposes today, we have traces taken from both ends of the TLS, encapsulating about a minute of a file copy

Using these two traces, we will *Draw the CNS Pie*, estimating how much time the Client contributes to this file copy, how much time the Network contributes, and how much time the Server contributes



Given the pie, we will then offer insights into what effect changing a component might have. For example, in the Pie on this page, we can see that shrinking the Network portion would not have much effect on overall transaction time – the place where we really want to put our attention is on the Server

Case 5: Making Pie

There are lots of ways to do this. I review a few in a paper called Making Client / Network / Server Pie http://www.skendric.com/app/

These techniques are all fragile – there are many ways in which they can go south and deliver misleading results

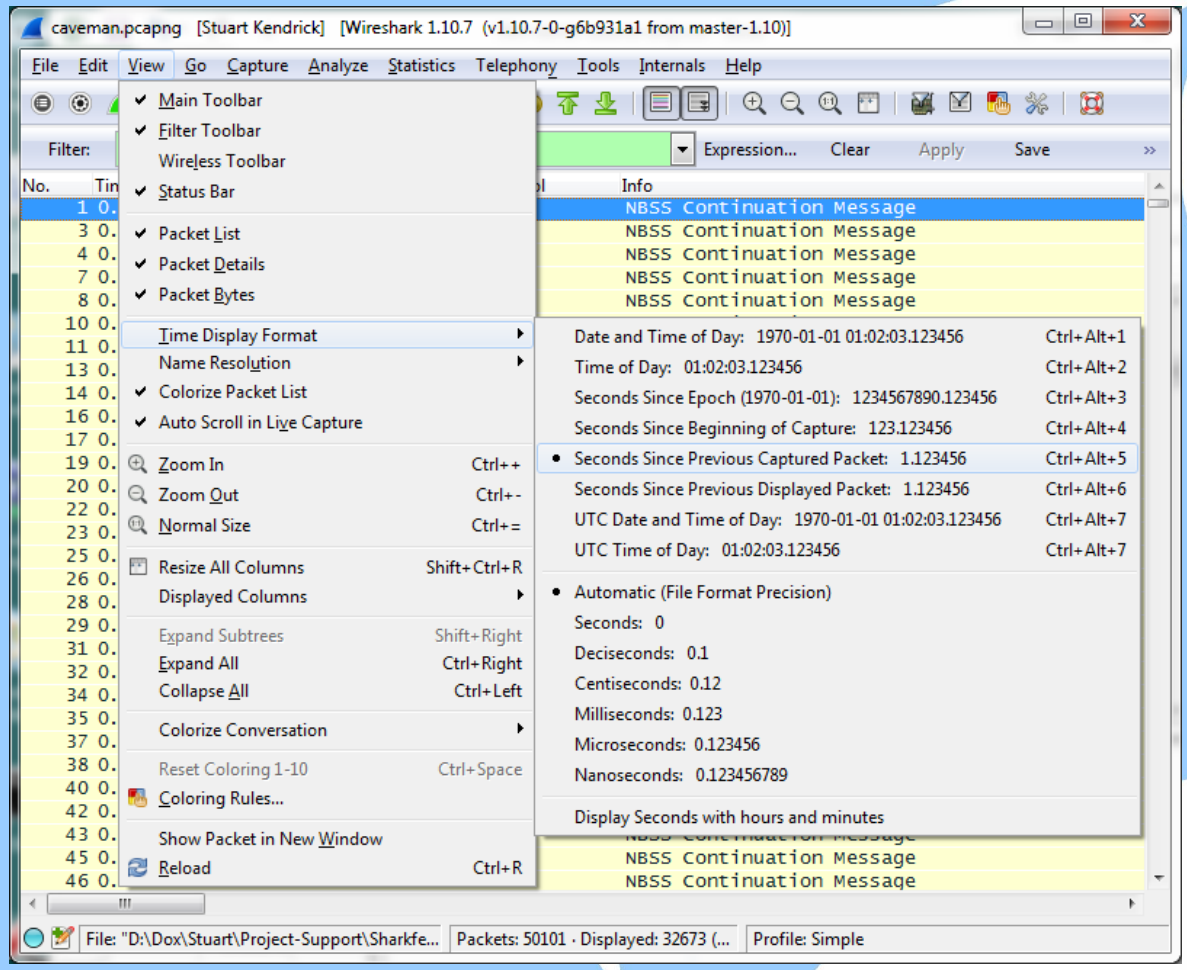
High-end applications, e.g *OpNet* et al, attempt to robustify this process – I've never used them, but I hear that they do a good job; though unsurprisingly, they can make mistakes also

There is no silver bullet

Let's dive into one of these techniques

Case 5: Client-Side View DeltaT

First, filter the Client-Side trace so that it contains only frames for a single conversation between Client and Server. Then, set the time column to DeltaT, aka Seconds Since Previous Captured Packet



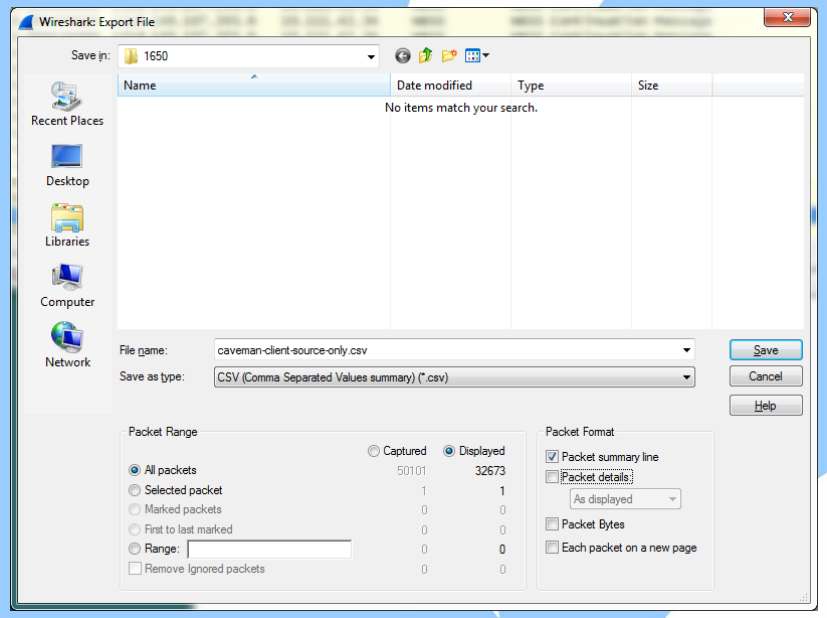
Case 5: Client-Side Extract DeltaT

Using the Client-Side trace, filter so that you see only the frames sourced from the Client

```
ip.src==a.b.c.d
```

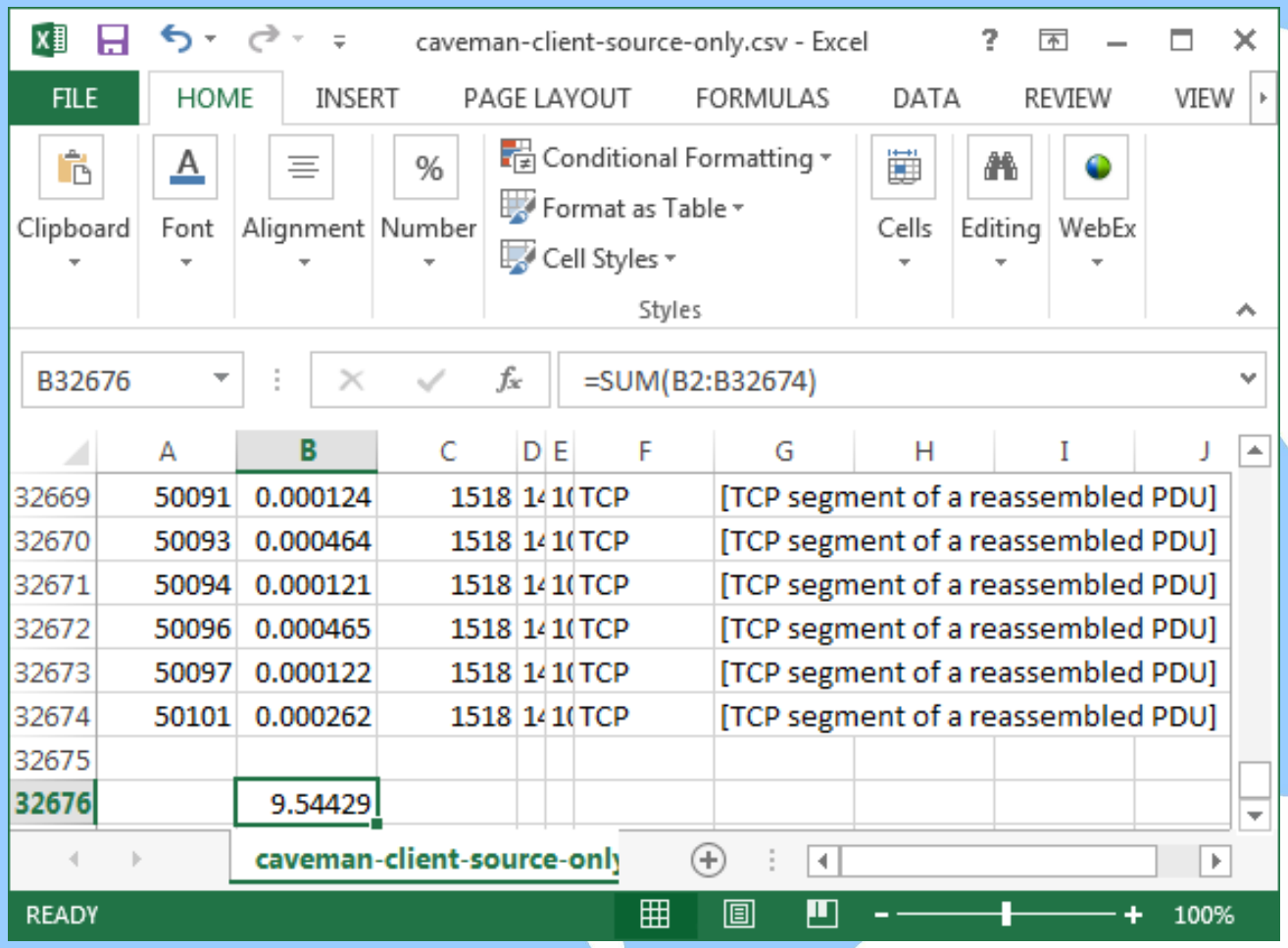
We want to sum the list of values in the Time column now. Why? Because the DeltaT value between each frame represents how long the Client spent thinking, before spitting out the next frame. If we sum all the time that the Client spent thinking, then we have an estimate for the Client's contribution to the Pie

Choose File.., Export Packet Dissections…, as CSV (Comma Separated Values packet summary) file and verify that only the Packet summary line box is checked



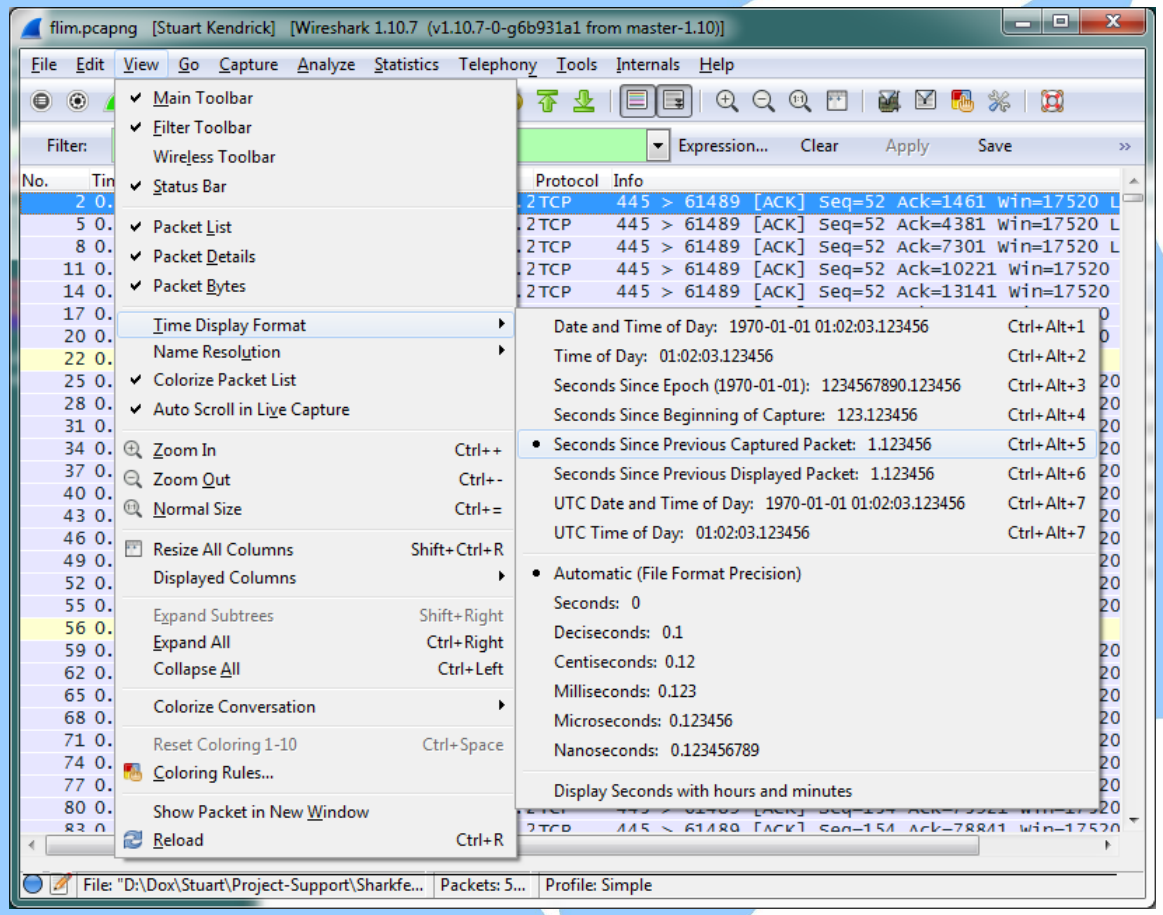
Case 5: Client-Side Sum DeltaT

Open the resulting file with a spreadsheet app, scroll to the bottom, and Sum the contents of the DeltaT column. Ahh, the Client's contribution is ~10s



Case 5: Server-Side View DeltaT

Now, filter the Server-Side trace so that it contains only frames for a single conversation between Client and Server. Then, set the time column to DeltaT, aka Seconds Since Previous Captured Packet



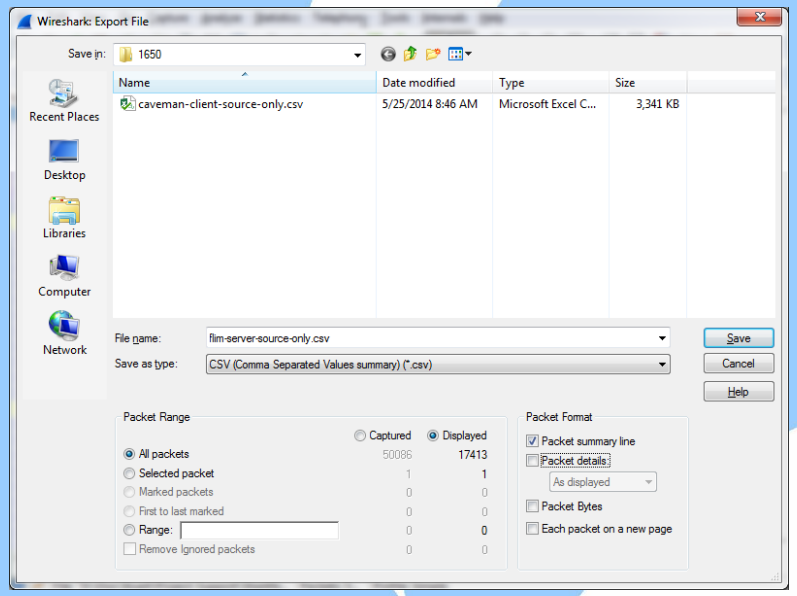
Case 5: Server-Side Extract DeltaT

Using the Server-Side trace, filter so that you see only the frames sourced from the Server

```
ip.src==e.f.g.h
```

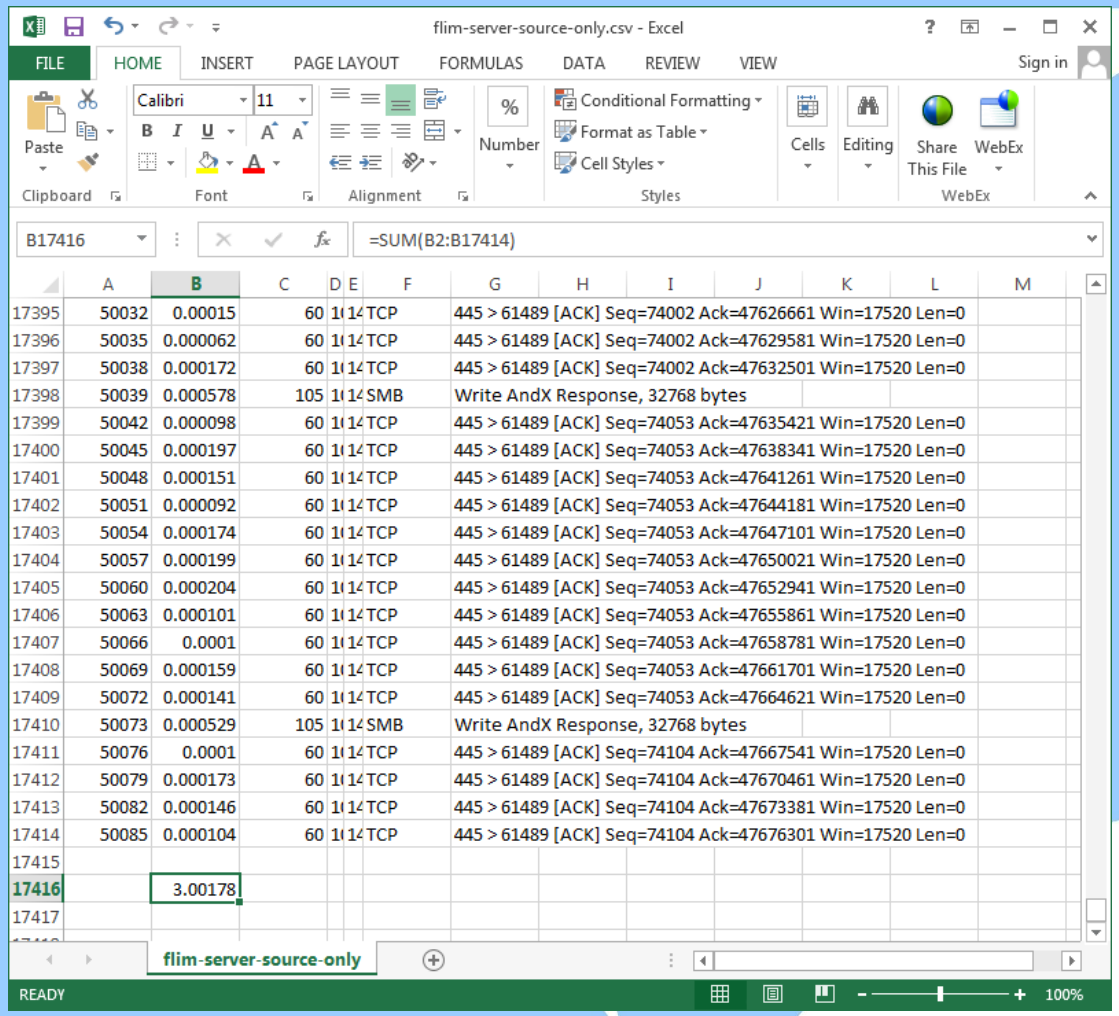
We want to sum the list of values in the Time column now. Why? Because the DeltaT value between each frame represents how long the Server spent thinking, before spitting out the next frame. If we sum all the time that the Server spent thinking, then we have an estimate for the Server's contribution to the Pie. [Perspicacious readers will notice that the Server side trace in this case study wasn't taken precisely next to the Server … but let's ignore this for now.]

Choose File.., Export Packet Dissections…, as CSV (Comma Separated Values packet summary) file and verify that only the Packet summary line box is checked



Case 5: Server-Side Sum DeltaT

Open the resulting file with a spreadsheet app, scroll to the bottom, and Sum the contents of the DeltaT column. Ahh, the Server's contribution is ~3s



	A	B	C	D	E	F	G
17395	50032	0.00015	60	1	14	TCP	445 > 61489 [ACK] Seq=74002 Ack=47626661 Win=17520 Len=0
17396	50035	0.000062	60	1	14	TCP	445 > 61489 [ACK] Seq=74002 Ack=47629581 Win=17520 Len=0
17397	50038	0.000172	60	1	14	TCP	445 > 61489 [ACK] Seq=74002 Ack=47632501 Win=17520 Len=0
17398	50039	0.000578	105	1	14	SMB	Write AndX Response, 32768 bytes
17399	50042	0.000098	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47635421 Win=17520 Len=0
17400	50045	0.000197	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47638341 Win=17520 Len=0
17401	50048	0.000151	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47641261 Win=17520 Len=0
17402	50051	0.000092	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47644181 Win=17520 Len=0
17403	50054	0.000174	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47647101 Win=17520 Len=0
17404	50057	0.000199	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47650021 Win=17520 Len=0
17405	50060	0.000204	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47652941 Win=17520 Len=0
17406	50063	0.000101	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47655861 Win=17520 Len=0
17407	50066	0.0001	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47658781 Win=17520 Len=0
17408	50069	0.000159	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47661701 Win=17520 Len=0
17409	50072	0.000141	60	1	14	TCP	445 > 61489 [ACK] Seq=74053 Ack=47664621 Win=17520 Len=0
17410	50073	0.000529	105	1	14	SMB	Write AndX Response, 32768 bytes
17411	50076	0.0001	60	1	14	TCP	445 > 61489 [ACK] Seq=74104 Ack=47667541 Win=17520 Len=0
17412	50079	0.000173	60	1	14	TCP	445 > 61489 [ACK] Seq=74104 Ack=47670461 Win=17520 Len=0
17413	50082	0.000146	60	1	14	TCP	445 > 61489 [ACK] Seq=74104 Ack=47673381 Win=17520 Len=0
17414	50085	0.000104	60	1	14	TCP	445 > 61489 [ACK] Seq=74104 Ack=47676301 Win=17520 Len=0
17415							
17416		3.00178					
17417							

Case 5: Total Time

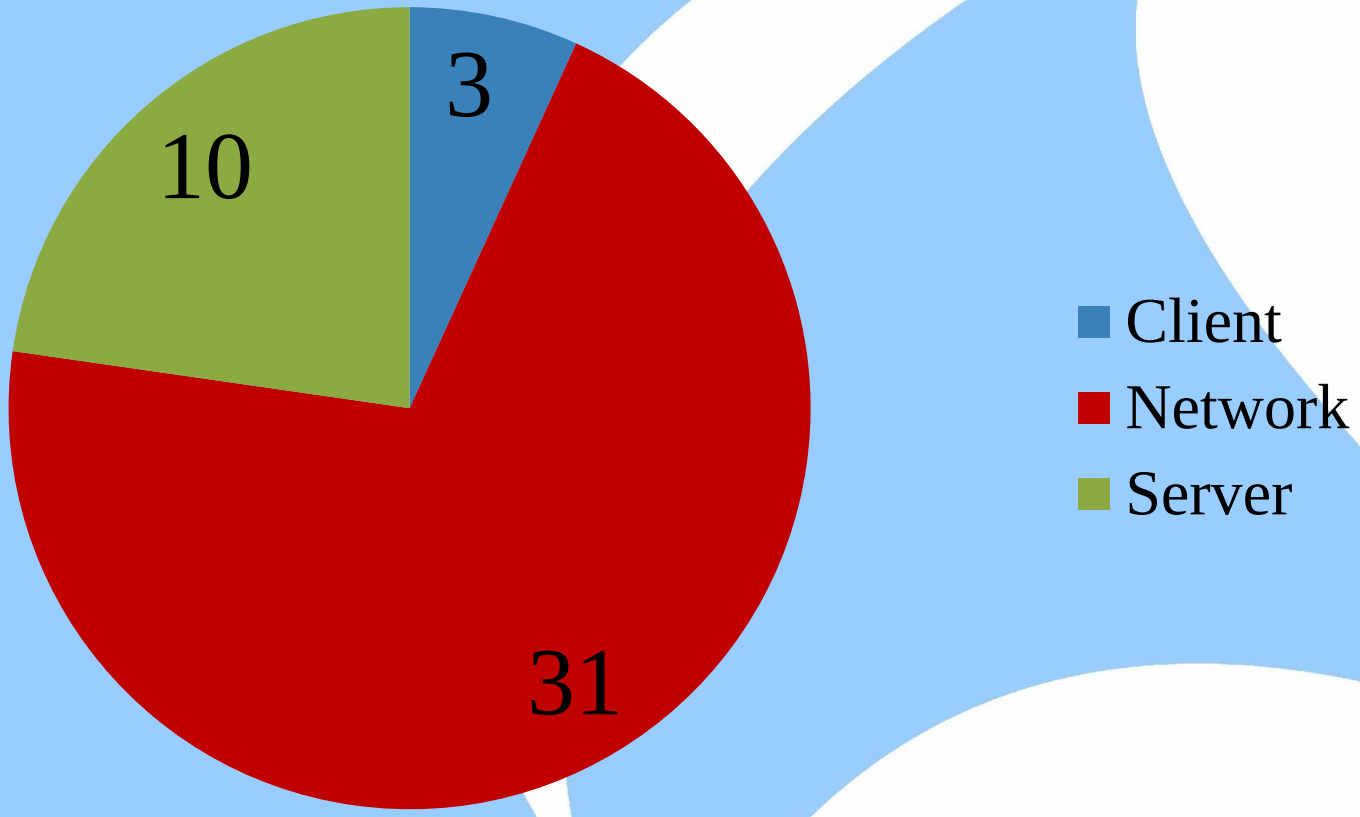
How much time total do these traces cover? Go to the Statistics menu, Summary, and look for Time / Elapsed. Or use the Wireshark *capinfos.exe* utility:

```
C:\Temp> capinfos caveman.pcapng
File name:           caveman.pcapng
File type:           Wireshark/... - pcapng
File encapsulation:  Ethernet
Packet size limit:   file hdr: (not set)
Number of packets:   50 k
File size:           52 MB
Data size:           50 MB
Capture duration:    44 seconds
Start time:          Wed Apr 10 16:48:59 2013
End time:            Wed Apr 10 16:49:44 2013
Data byte rate:      1149 kBps
Data bit rate:       9197 kbps
Average packet size: 1013.07 bytes
Average packet rate: 1134 packets/sec
SHA1:                e6461c3ef2cb009beb048706e89b8248f587b228
RIPEMD160:           da28a8dac1d756a6f439d443636d96a0319d3254
MD5:                 bf6d59e8cd1d28e10fbef47718012980
Strict time order:   True
```

Case 5: Draw the Pie

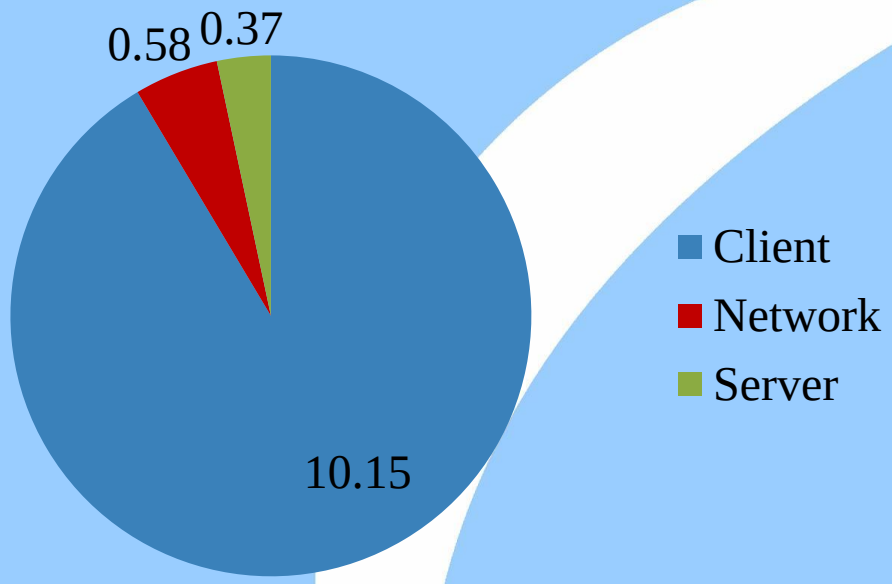
OK, so the Client consumed ~10s, the Server consumed ~3s: how much time did the Network consume?

```
44s - 10s - 3s = 31s
```



Case 5: Draw More Pies

If we repeat this for other applications, we find, for example, that for browsing Internet Web sites, the pie looked liked this. Hard to believe? Turns out the Client was struggling with not enough memory.



The Outlook pie looked rather like the one above, while browsing Internal Web sites split the time more evenly between the three components.

Case 5: Your Story

How would you tell this story?

Will upgrading the TLS to 100Mb make a difference, and if so, by how much?

Thank you!

On-Line Resources

Rapid Problem Resolution by Paul Offord
LinkedIn Protocol Analysis & Troubleshooting Group
Old Comm Guy http://www.lovemytool.com

Trouble-shooting & Training Outfits		**Based Here (will travel for $$)**
James Baxter	http://www.packetiq.com	Daytona Beach, FL
Tony Fortunato	http://www.thetechfirm.com	Toronto, Canada
Chris Greer	http://www.packetpioneer.com	Central/South America
Paul Offord	http://www.advance7.com	London (international)
Mike Pennacchi	http://www.nps-llc.com	Seattle, WA
Ray Tompkins	http://www.gearbit.com	Austin, TX
…		

Conferences

Sharkfest	http://sharkfest.wireshark.org	San Francisco, CA

Follow-up stuart.kendrick.sea {at} gee mail dot com
This deck visible at http://www.skendric.com/seminar