The Art of Debugging
Using a network sniffer to isolate hardware, software, systems, and interoperability problems

David A. Soussan
Chief Engineer
DAS Computer Consultants, Ltd.

Microsoft®

Today's Presenter

David A. Soussan, DAS Computer Consultants
Birmingham, Michigan
Self-proclaimed über-geek

- MCP from back in the NT4 days
- BSCS, 30+ years in the computer field
- 2005 "Windows IT Pro Innovator of the Year"

E-mail: webcast@dascc.com

Microsoft

Goals

- Add a new tool to your tool belt, or use an existing tool in new ways
- Become a better debugger / problem solver
- See some common faults and where to look
- Touch on “But wait! There’s more!”

Microsoft

Prerequisites

- Networking
- Protocols (TCP, DNS, ICMP, TFTP…)
- Software (touch of Microsoft® Visual Basic®, Microsoft® SQL Server™)
- 200-400 level material

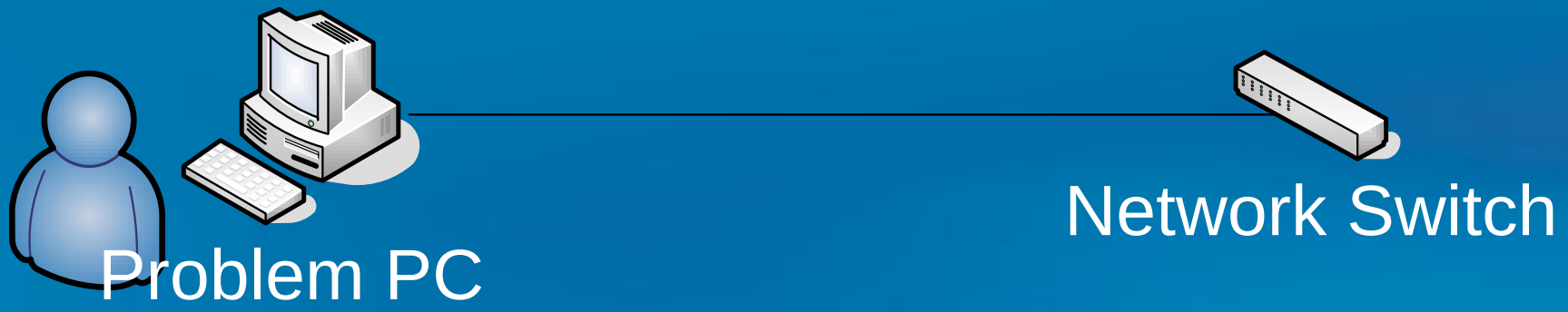
Microsoft®

What We Will Cover

- Sniffing – what it is and why
- Tools we'll use today and how
- Screen shots in the slide deck are for later reference highlighting relevant data
- Maximize analysis of real customer problems with saved data from 8+ scenarios
- Request for comments (RFCs) for more protocol understanding
- Where to get more information and tools

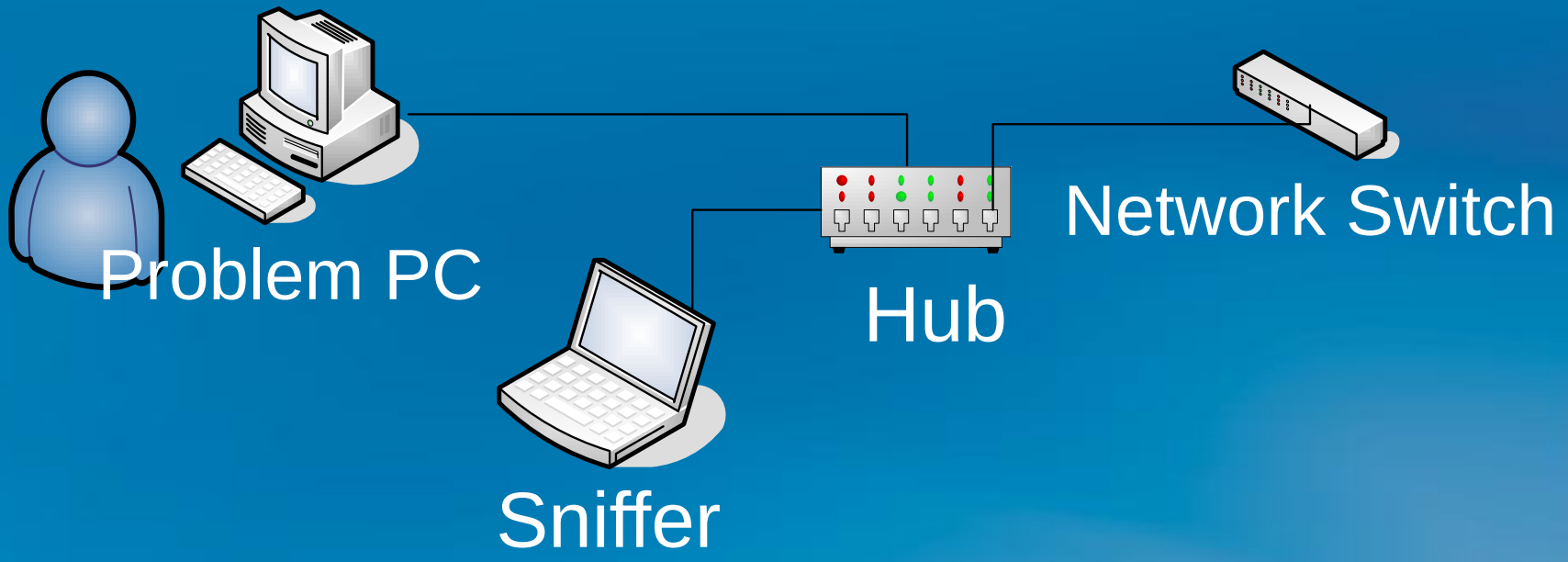
Microsoft

Sniffing?



Sniffing?

Sniffing?



General Process

- Pick an interesting spot on the network
- Connect sniffer
- Make fault happen
- Filter capture on what is interesting
- Interpret what exactly happened

Microsoft

Ethereal (Now Wireshark)

- Powerful
- Multiplatform
- FREE!
- Other tools: Microsoft® Network Monitor (NetMon), Network Monitor for Microsoft® Systems Management Server, snoop, Network General, Fluke OptiView…

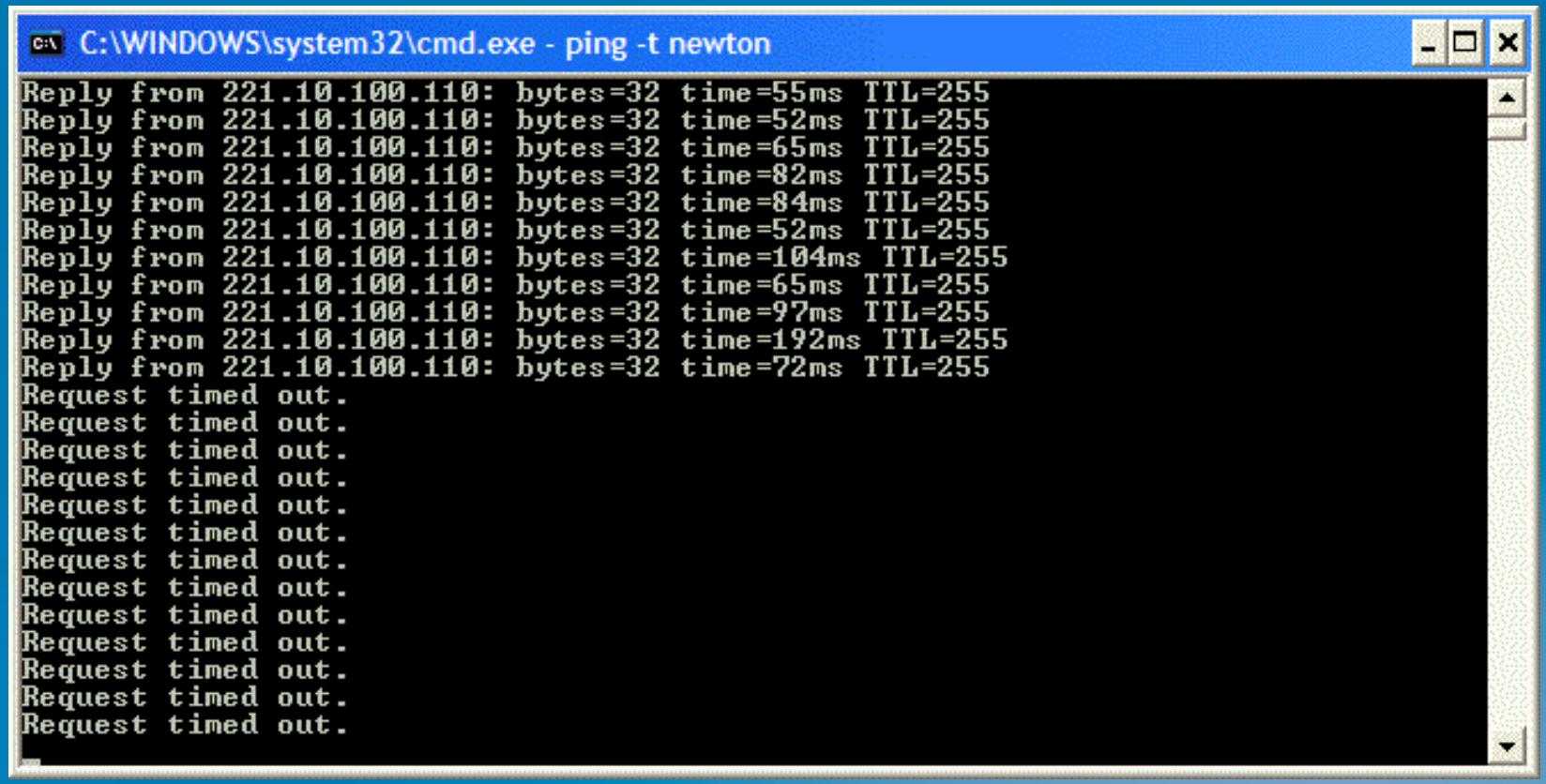
Microsoft®

Scenarios to Cover

- Intermittent Internet connectivity
- Intermittent Internet connectivity – 2
- “Is my girlfriend spying on me?”
- NT2K domain with intermittent Internet problems, client wants wiring certified
- Windows® CE TFTP boot failure
- Malicious software (malware) infection
- Very large system problem (Visual Basic, Informix, Sun Solaris, OC-48, Microwave, OS-9, …)
- Slow FTP @ 100 Mb/s, fast at 10 Mb/s
- FTP failures

Microsoft®

Scenario One

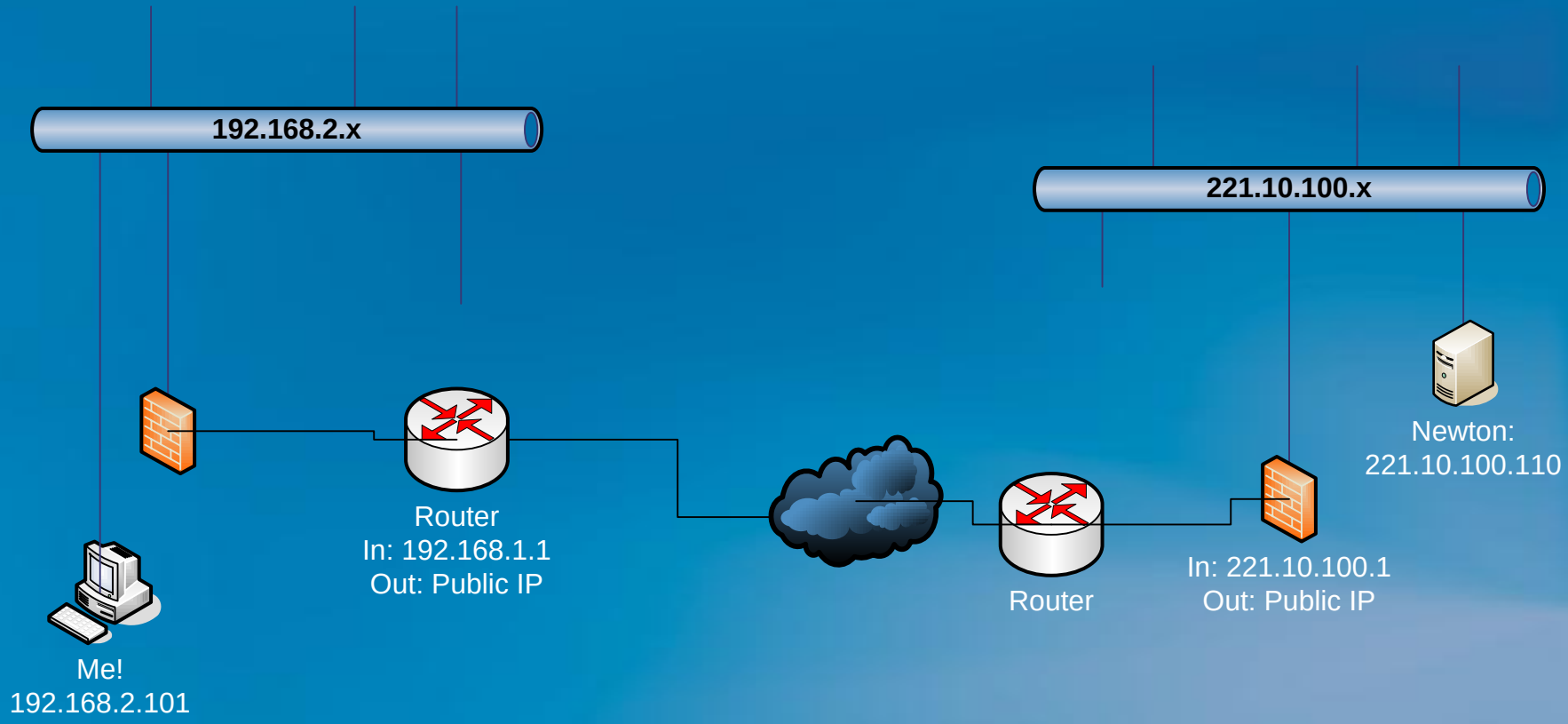


Intermittent Network Connectivity One

Microsoft

A Troubled Network

Intermittent Internet Connectivity



Microsoft

Demonstration One

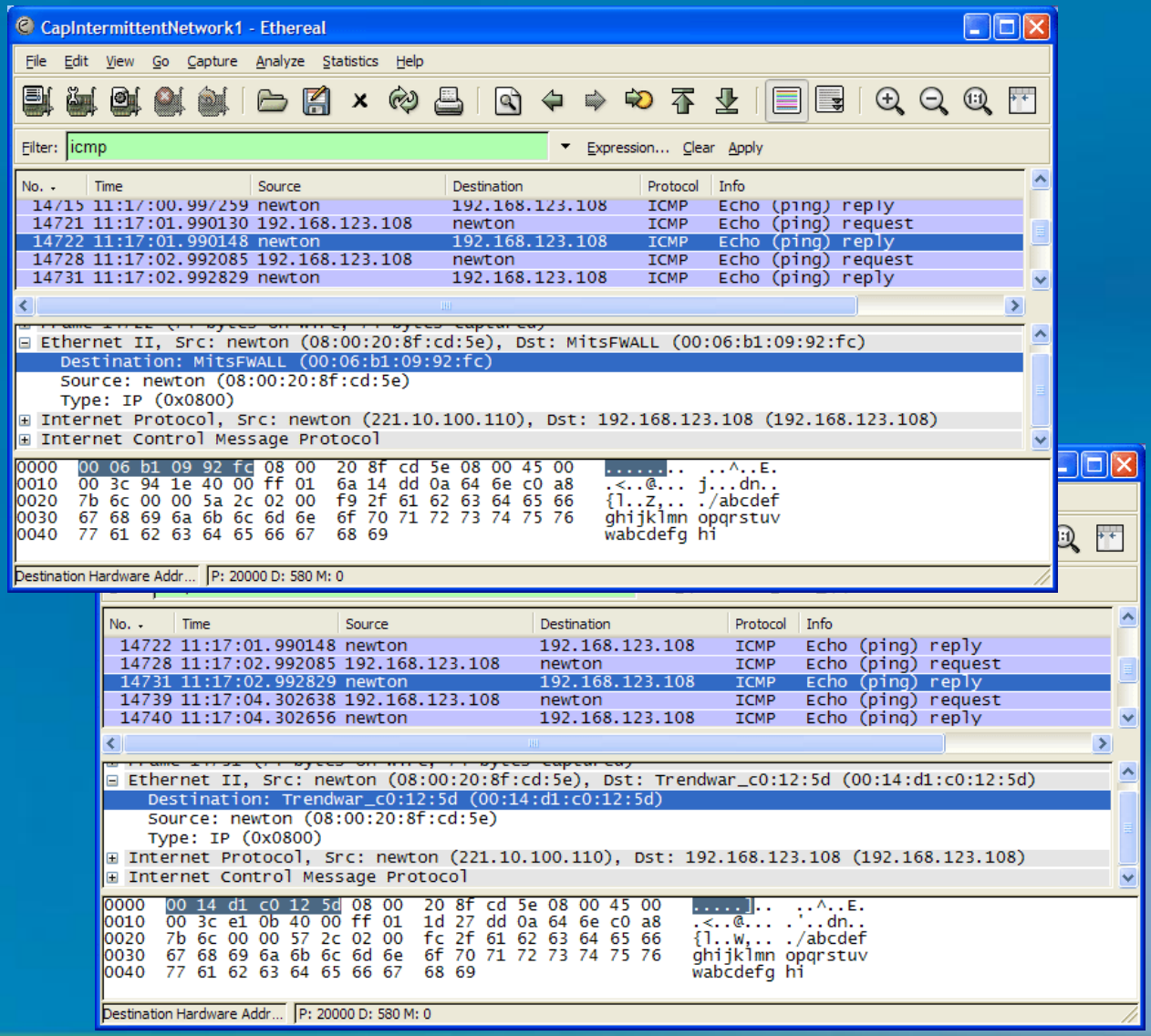
demo

Intermittent Internet One

The actual data sniff in Ethereal!

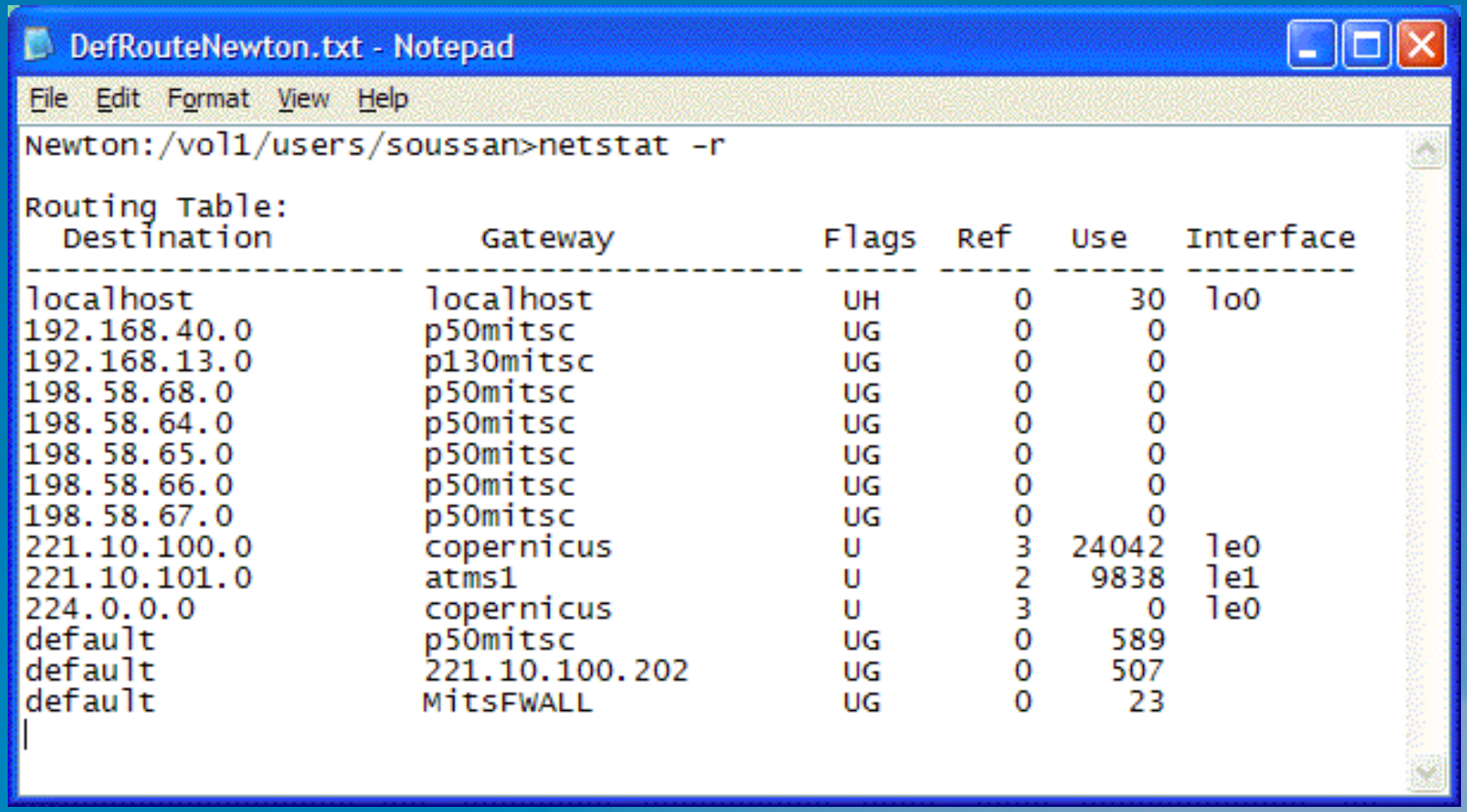
Microsoft®

Finding the Mystery Router



Microsoft

Newton's Routing Table


DefRouteNewton.txt - Notepad

File Edit Format View Help

```
Newton:/vol1/users/soussan>netstat -r

Routing Table:
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
localhost            localhost             UH        0      30  lo0
192.168.40.0         p50mitsc              UG        0       0
192.168.13.0         p130mitsc             UG        0       0
198.58.68.0          p50mitsc              UG        0       0
198.58.64.0          p50mitsc              UG        0       0
198.58.65.0          p50mitsc              UG        0       0
198.58.66.0          p50mitsc              UG        0       0
198.58.67.0          p50mitsc              UG        0       0
221.10.100.0         copernicus            U         3   24042  le0
221.10.101.0         atms1                 U         2    9838  le1
224.0.0.0            copernicus            U         3       0  le0
default              p50mitsc              UG        0     589
default              221.10.100.202        UG        0     507
default              MitsFWALL             UG        0      23
```

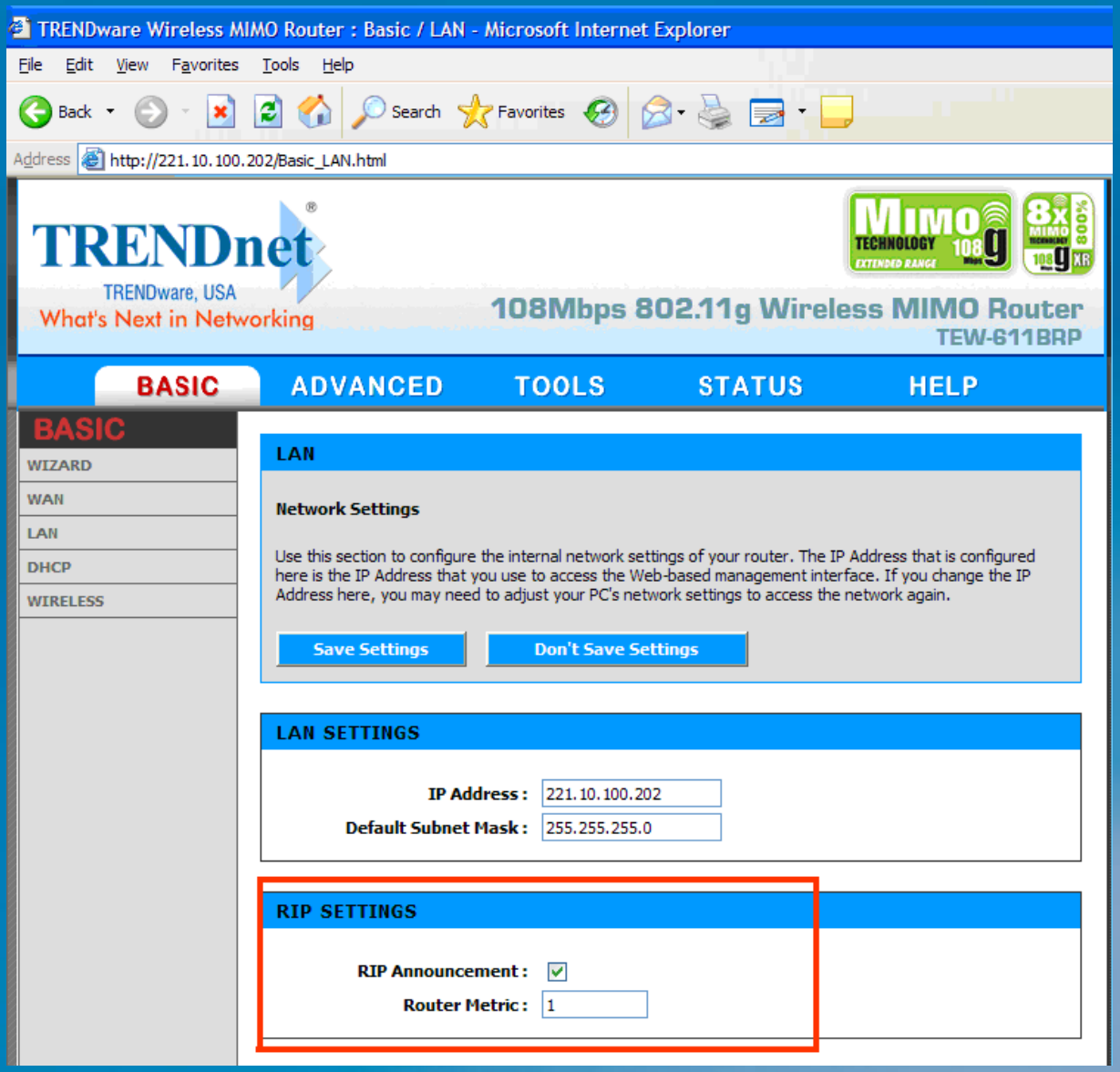

Microsoft

Every Network Device Routes!

```
C:\temp>route print
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1   192.168.2.175       25
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      192.168.2.0    255.255.255.0    192.168.2.175   192.168.2.175       25
    192.168.2.175  255.255.255.255        127.0.0.1       127.0.0.1       25
    192.168.2.255  255.255.255.255    192.168.2.175   192.168.2.175       25
        224.0.0.0        240.0.0.0    192.168.2.175   192.168.2.175       25
  255.255.255.255  255.255.255.255    192.168.2.175   192.168.2.175        1
  255.255.255.255  255.255.255.255    192.168.2.175               2        1
Default Gateway:       192.168.2.1
===========================================================================
Persistent Routes:
  None
```

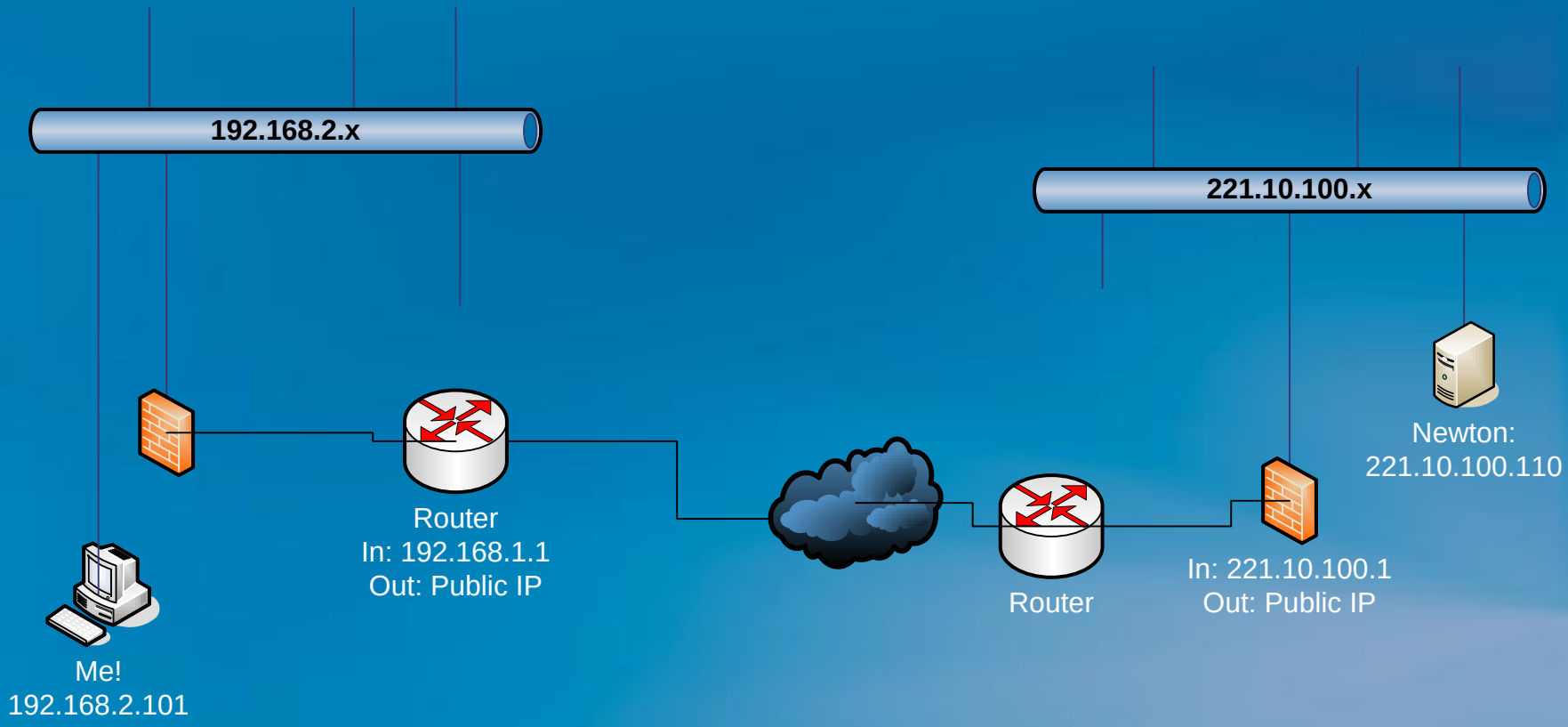
```
IP gateway (route) table:
0. Default Gateway -> PPP (pppoe/vcc1), D 2, T 0, (configured) UP DEFAULT

IP route cache (108 entries):
Net 70.233.1.149 gateway 70.233.1.149 metric 0 timeout 5 via ENET (10/100BT-LAN)
Net 70.233.1.151 broadcast via ENET (10/100BT-LAN)
Net 70.233.1.254 broadcast via PPP (pppoe/vcc1)
Net 87.10.191.244 point-to-point metric 0 timeout 1 via PPP (pppoe/vcc1)
Net 75.184.113.21 point-to-point metric 0 timeout 3 via PPP (pppoe/vcc1)
Net 68.114.167.30 point-to-point metric 0 timeout 4 via PPP (pppoe/vcc1)
Net 72.67.106.30 point-to-point metric 0 timeout 4 via PPP (pppoe/vcc1)
```

What Is 221.10.100.202?



Network: Before

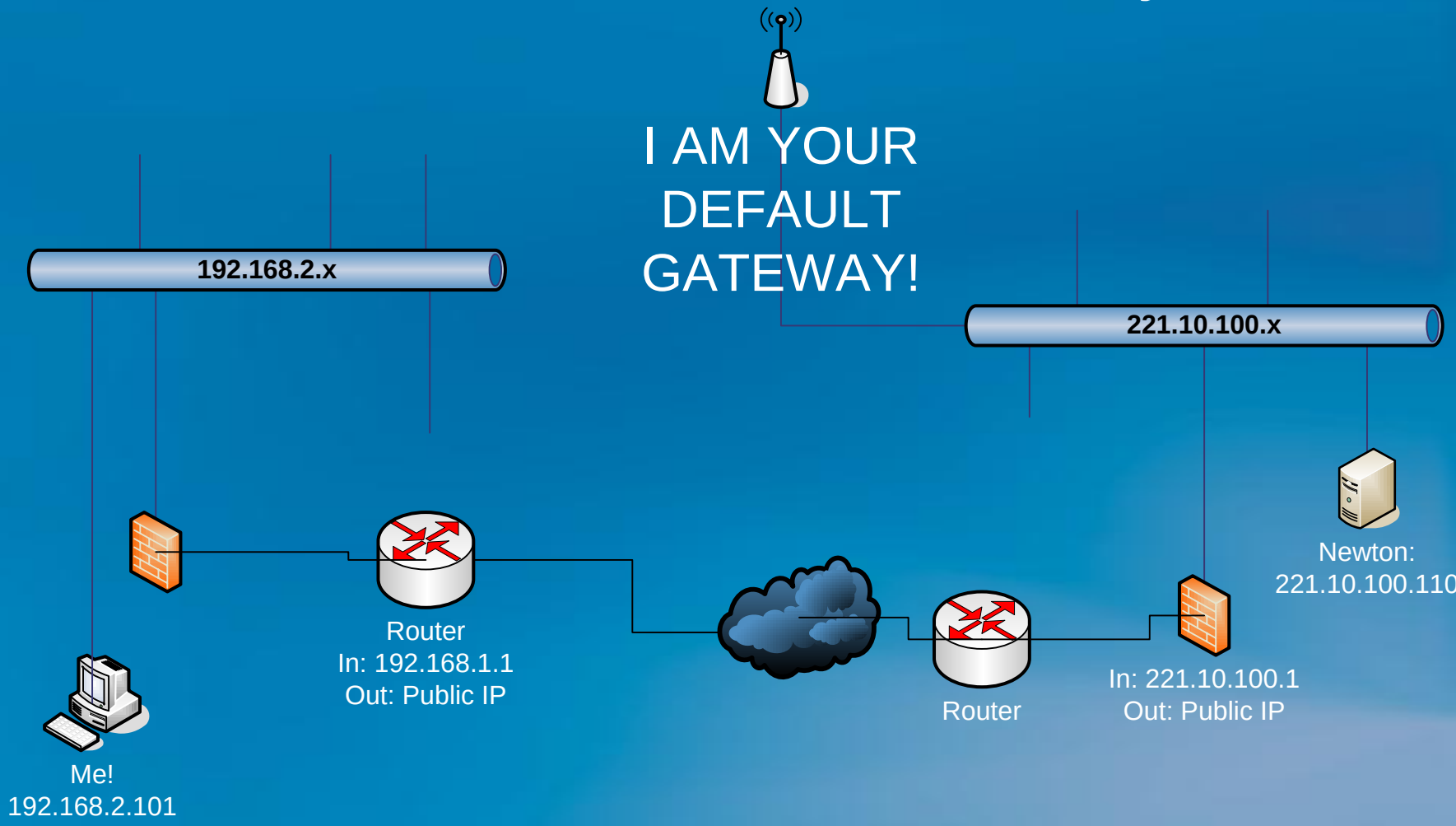
Intermittent Internet Connectivity



Microsoft

Network: After (Broken)

Intermittent Internet Connectivity



Microsoft

Demonstration Two

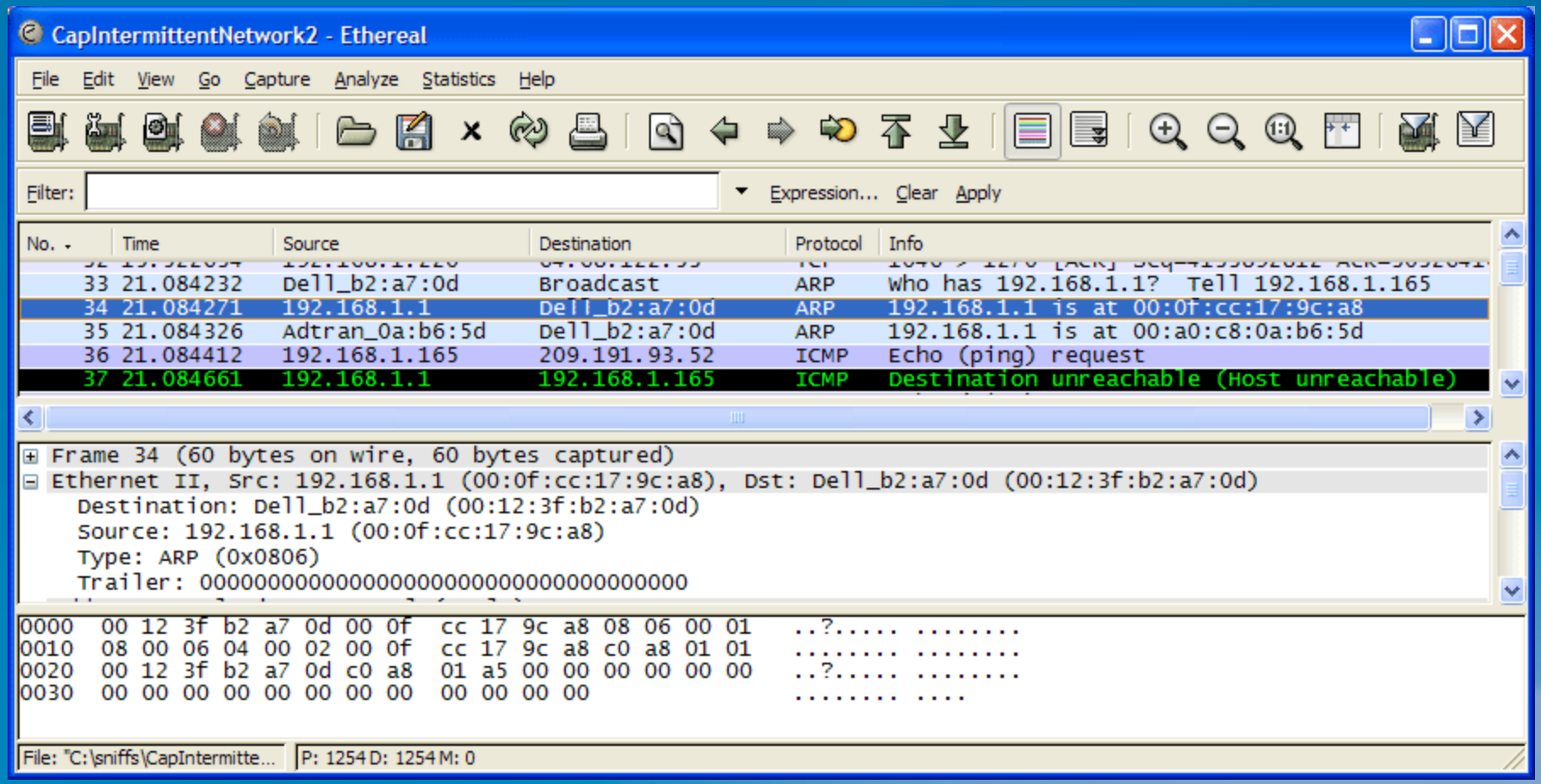
demo

Intermittent Internet Two

Exact same symptom, different root cause

Microsoft®

Intermittent Internet Two



Microsoft

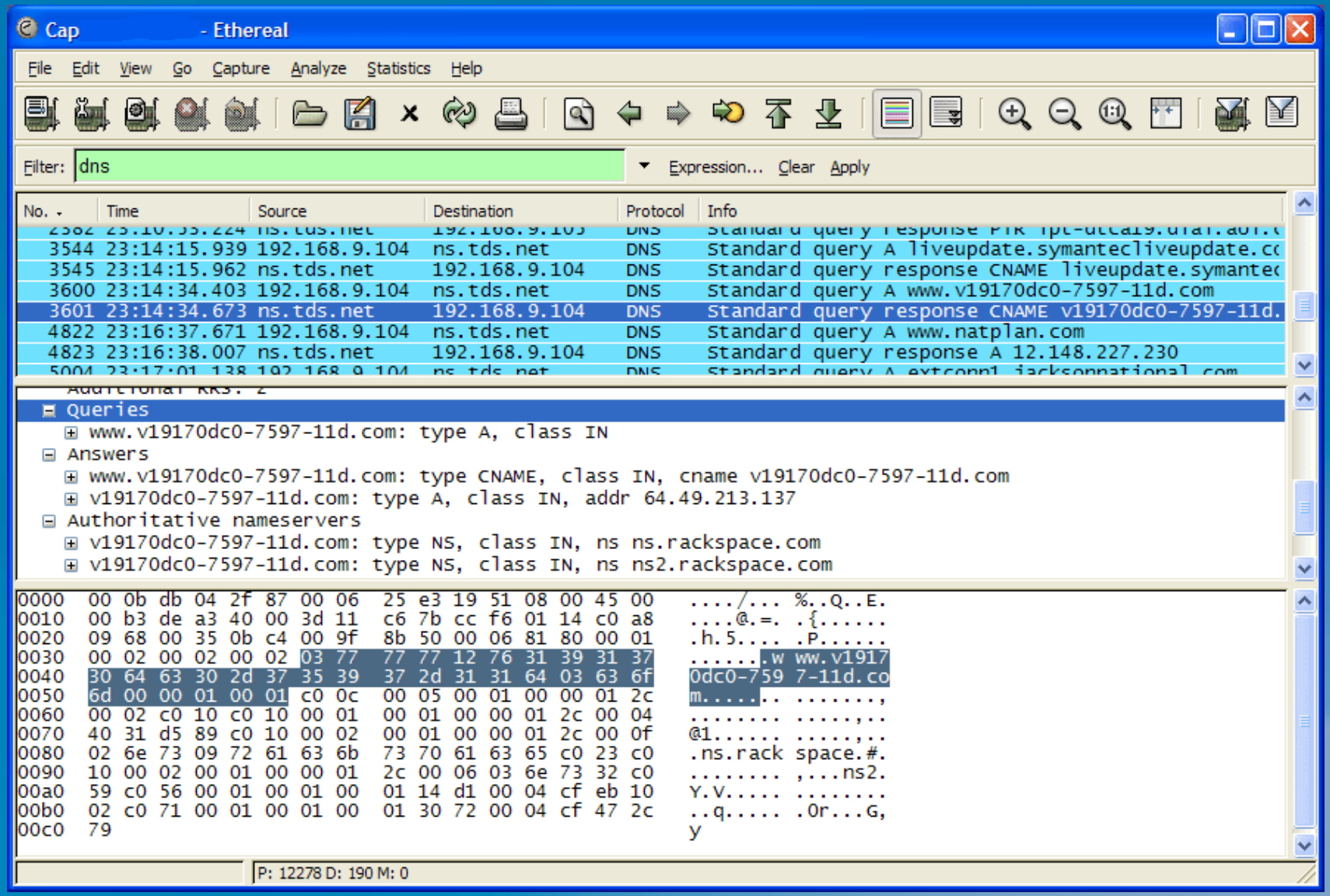
Demonstration Three

demo

"How can she possibly know everything I'm doing????"

Microsoft®

Filtered on DNS Queries



Whois v19170dc0-7597-11d.com

```
c:\temp > whois V19170DC0-7597-11D.COM
Whois Server Version 2.0

   Domain Name: V19170DC0-7597-11D.COM
   Registrar: DSTR ACQUISITION VII, LLC
   Updated Date: 21-feb-2006

Registrant:
   Spectorsoft Corp. (V19170DC0-7597-11D-COM-DOM)
   1555 Indian River Blvd
   Bldg B-210
   Vero Beach, FL 32960
   U.S.
   info@spectorsoft.com

   Domain Name: V19170DC0-7597-11D.COM
```

Spectorsoft?

Demonstration Four

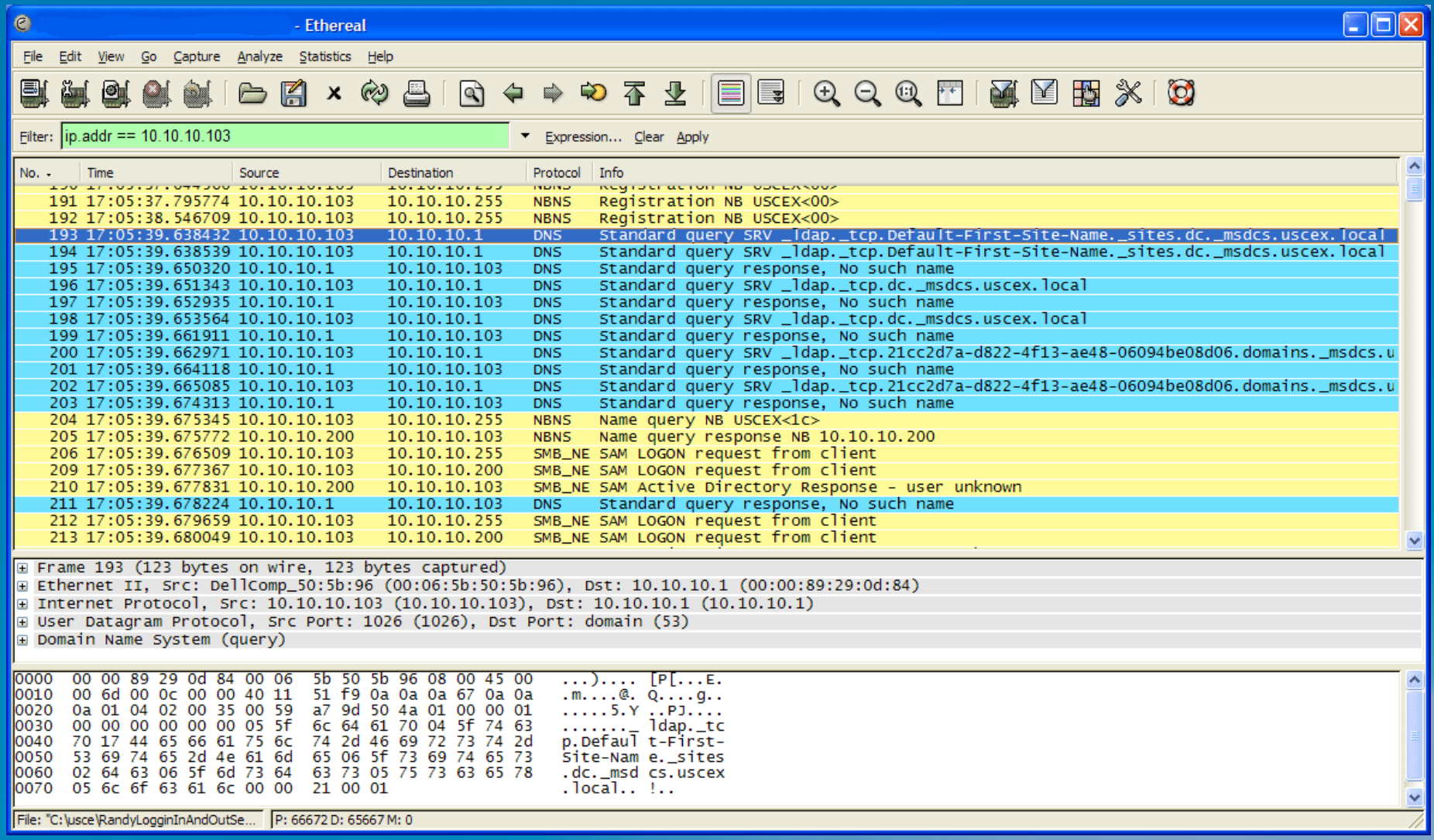
demo

Slow boot, net share disconnections, wiring problems

Do we follow customer's recommendations, or not?

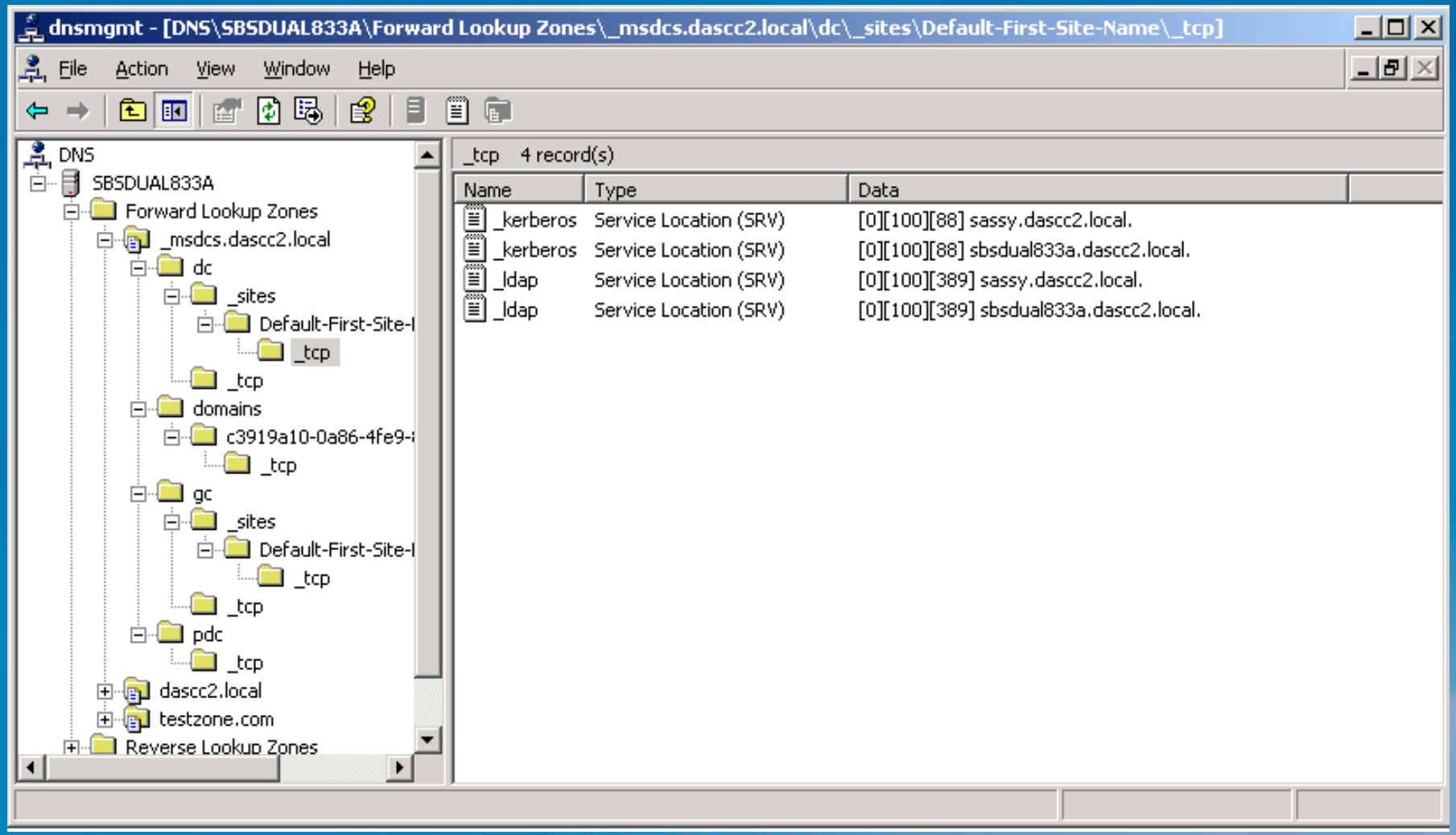
Microsoft®

Active Directory* DNS to Wrong Server



* Active Directory® directory service

What DNS Should Look Like



Microsoft

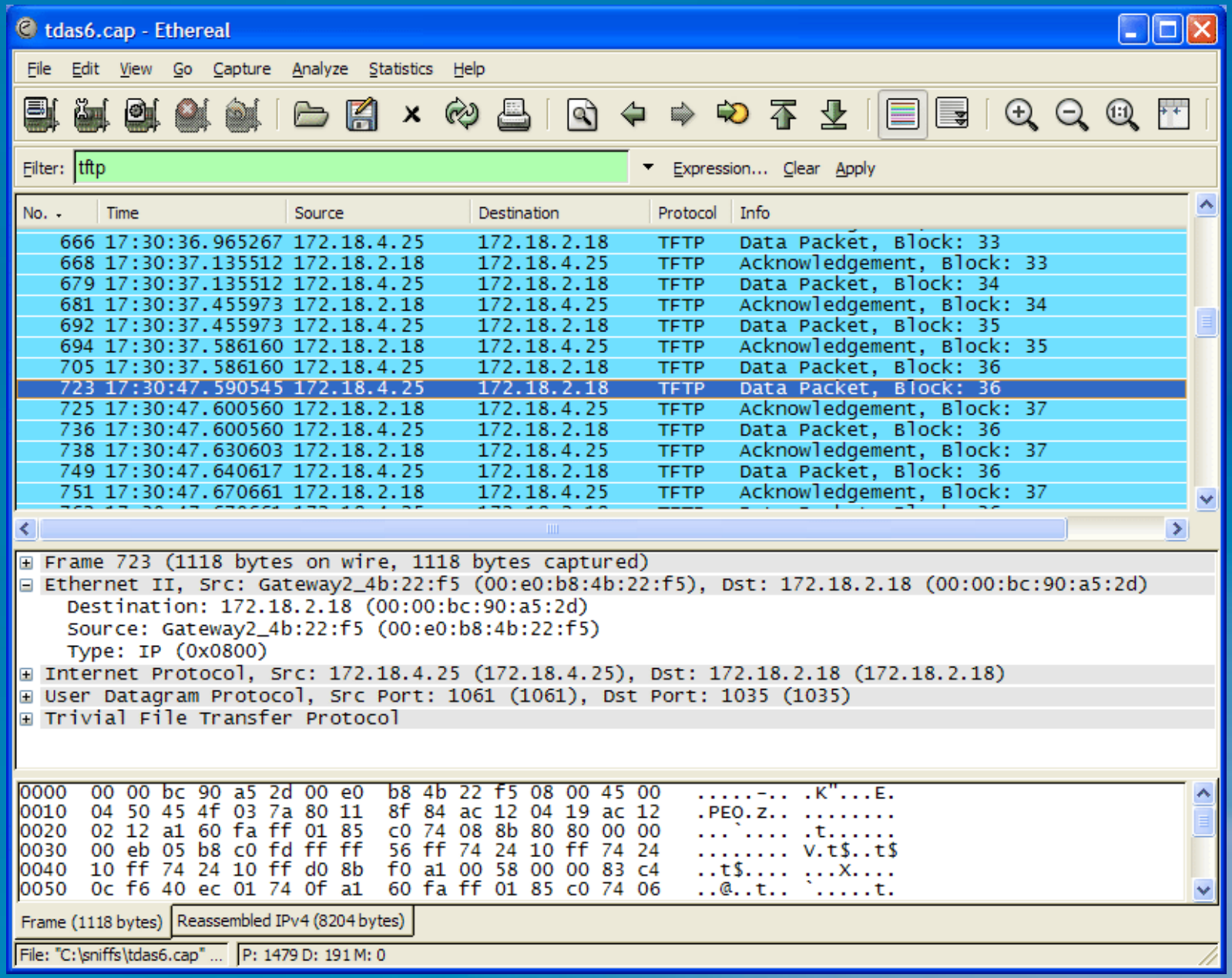
Demonstration Five

demo

TFTP Boot Failure

4 Processors:
3 AMDs booting Windows CE
1 ARM OS-9K serving files to the 3 AMDs
All inside one box in an airplane

Microsoft®


tdas6.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: tftp
Expression... Clear Apply
No. Time Source Destination Protocol Info
666 17:30:36.965267 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 33
668 17:30:37.135512 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 33
679 17:30:37.135512 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 34
681 17:30:37.455973 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 34
692 17:30:37.455973 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 35
694 17:30:37.586160 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 35
705 17:30:37.586160 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 36
723 17:30:47.590545 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 36
725 17:30:47.600560 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 37
736 17:30:47.600560 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 36
738 17:30:47.630603 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 37
749 17:30:47.640617 172.18.4.25 172.18.2.18 TFTP Data Packet, Block: 36
751 17:30:47.670661 172.18.2.18 172.18.4.25 TFTP Acknowledgement, Block: 37
Frame 723 (1118 bytes on wire, 1118 bytes captured)
Ethernet II, Src: Gateway2_4b:22:f5 (00:e0:b8:4b:22:f5), Dst: 172.18.2.18 (00:00:bc:90:a5:2d)
Destination: 172.18.2.18 (00:00:bc:90:a5:2d)
Source: Gateway2_4b:22:f5 (00:e0:b8:4b:22:f5)
Type: IP (0x0800)
Internet Protocol, Src: 172.18.4.25 (172.18.4.25), Dst: 172.18.2.18 (172.18.2.18)
User Datagram Protocol, Src Port: 1061 (1061), Dst Port: 1035 (1035)
Trivial File Transfer Protocol
0000 00 00 bc 90 a5 2d 00 e0 b8 4b 22 f5 08 00 45 00 .....-.. .K"...E.
0010 04 50 45 4f 03 7a 80 11 8f 84 ac 12 04 19 ac 12 .PEO.z.. ....
0020 02 12 a1 60 fa ff 01 85 c0 74 08 8b 80 80 00 00 ...`.... .t......
0030 00 eb 05 b8 c0 fd ff ff 56 ff 74 24 10 ff 74 24 .... V.t$..t$
0040 10 ff 74 24 10 ff d0 8b f0 a1 00 58 00 00 83 c4 ..t$.... ...X....
0050 0c f6 40 ec 01 74 0f a1 60 fa ff 01 85 c0 74 06 ..@..t.. `.....t.
Frame (1118 bytes)
Reassembled IPv4 (8204 bytes)
File: "C:\sniffs\tdas6.cap" ...
P: 1479 D: 191 M: 0

Demonstration Six

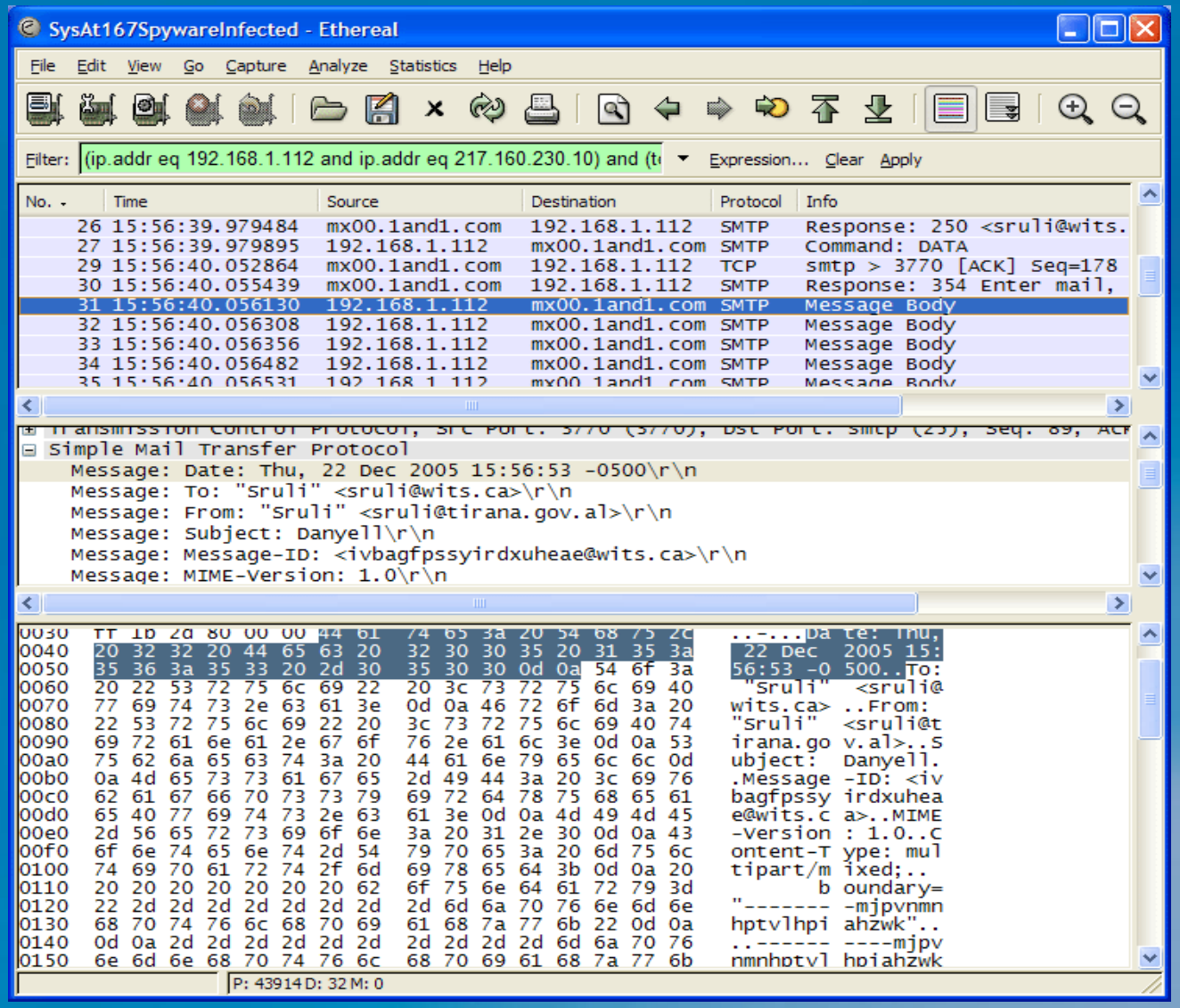
demo

Malware Infection

- Customer calls about pop-ups
- Drive-by issue on different system

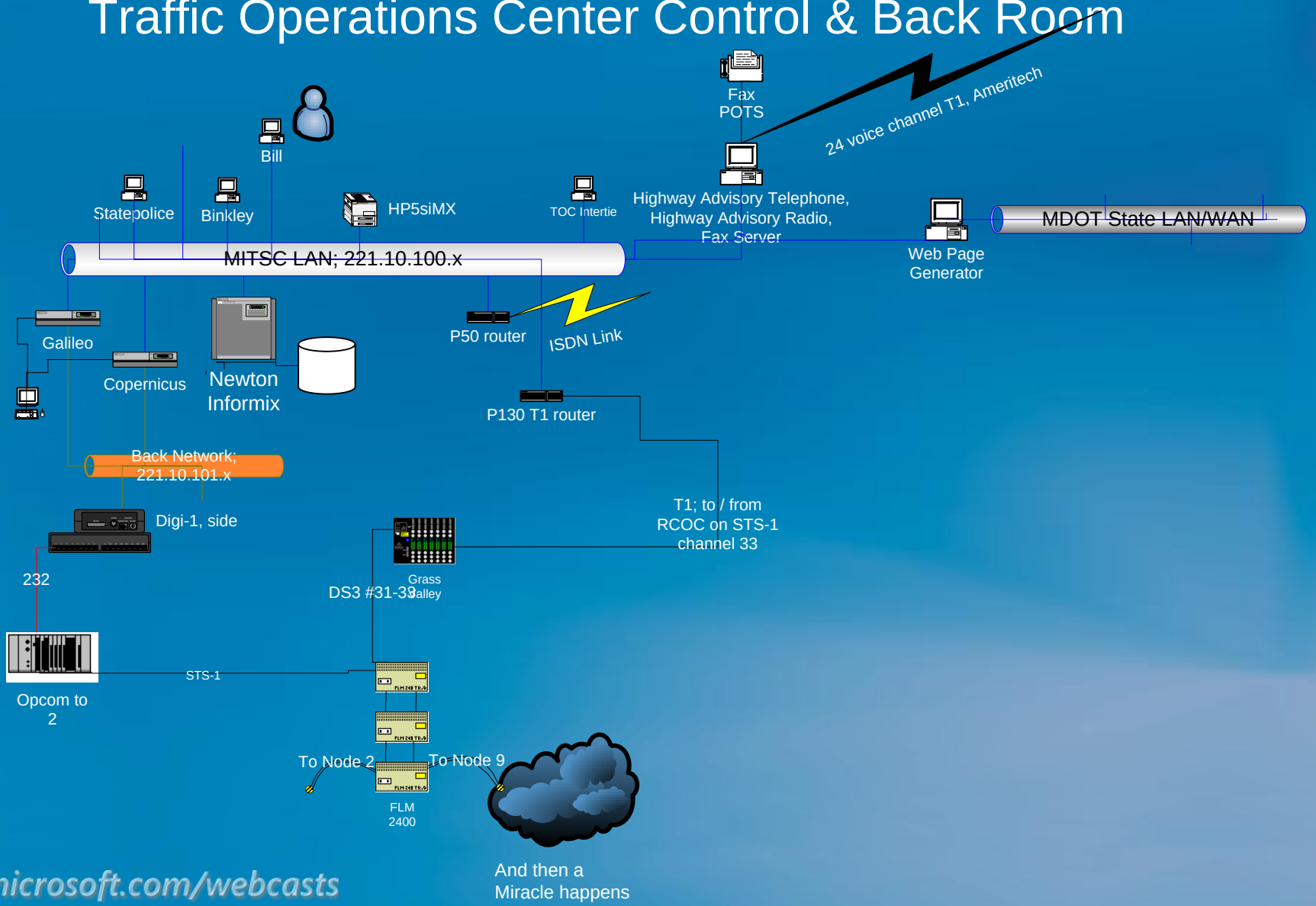
Microsoft®

Sending Viruses



Large System, Slow Updates

Traffic Operations Center Control & Back Room



And Then a Miracle Happens…

Finger Pointing Festival

- Visual Basic: “Informix too slow,” “Network too slow,” “Sun server too slow,” “Comm errors to field”
- Informix: “Server too slow,” “Need beefier hardware,” “Queries not optimal”
- Systems: “Visual Basic inefficient,” “Field communication errors,” “Upgrade net from 10 to 100 Mb/s,” “Unix daemons aren’t working properly”
- Field: “Field working fine, problem on your end”
- Unix: “Daemons are fine, NIMBY!”

Microsoft

Demonstration Seven

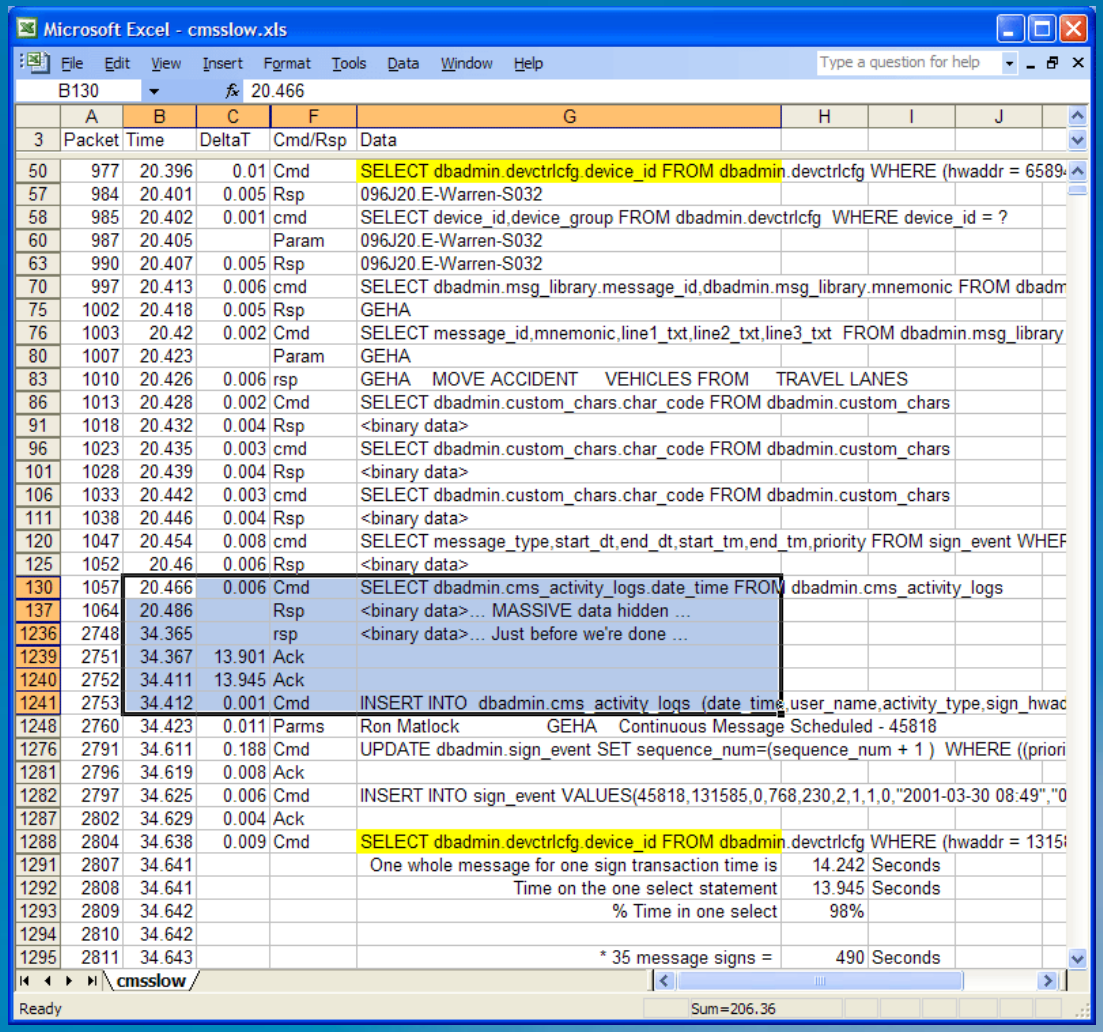
demo

Slow Sign Updates

- Very large, complex system

Microsoft®

Sniff and Build Message Sequence Diagram



Microsoft Excel - cmsslow.xls

File Edit View Insert Format Tools Data Window Help

B130 fx 20.466

	A	B	C	F	G	H	I	J
3	Packet	Time	DeltaT	Cmd/Rsp	Data			
50	977	20.396	0.01	Cmd	SELECT dbadmin.devctrlcfg.device_id FROM dbadmin.devctrlcfg WHERE (hwaddr = 6589			
57	984	20.401	0.005	Rsp	096J20.E-Warren-S032			
58	985	20.402	0.001	cmd	SELECT device_id,device_group FROM dbadmin.devctrlcfg WHERE device_id = ?			
60	987	20.405		Param	096J20.E-Warren-S032			
63	990	20.407	0.005	Rsp	096J20.E-Warren-S032			
70	997	20.413	0.006	cmd	SELECT dbadmin.msg_library.message_id,dbadmin.msg_library.mnemonic FROM dbadm			
75	1002	20.418	0.005	Rsp	GEHA			
76	1003	20.42	0.002	Cmd	SELECT message_id,mnemonic,line1_txt,line2_txt,line3_txt FROM dbadmin.msg_library			
80	1007	20.423		Param	GEHA			
83	1010	20.426	0.006	rsp	GEHA MOVE ACCIDENT VEHICLES FROM TRAVEL LANES			
86	1013	20.428	0.002	Cmd	SELECT dbadmin.custom_chars.char_code FROM dbadmin.custom_chars			
91	1018	20.432	0.004	Rsp	<binary data>			
96	1023	20.435	0.003	cmd	SELECT dbadmin.custom_chars.char_code FROM dbadmin.custom_chars			
101	1028	20.439	0.004	Rsp	<binary data>			
106	1033	20.442	0.003	cmd	SELECT dbadmin.custom_chars.char_code FROM dbadmin.custom_chars			
111	1038	20.446	0.004	Rsp	<binary data>			
120	1047	20.454	0.008	cmd	SELECT message_type,start_dt,end_dt,start_tm,end_tm,priority FROM sign_event WHEF			
125	1052	20.46	0.006	Rsp	<binary data>			
130	1057	20.466	0.006	Cmd	SELECT dbadmin.cms_activity_logs.date_time FROM dbadmin.cms_activity_logs			
137	1064	20.486		Rsp	<binary data>... MASSIVE data hidden ...			
1236	2748	34.365		rsp	<binary data>... Just before we're done ...			
1239	2751	34.367	13.901	Ack				
1240	2752	34.411	13.945	Ack				
1241	2753	34.412	0.001	Cmd	INSERT INTO dbadmin.cms_activity_logs (date_time,user_name,activity_type,sign_hwac			
1248	2760	34.423	0.011	Parms	Ron Matlock GEHA Continuous Message Scheduled - 45818			
1276	2791	34.611	0.188	Cmd	UPDATE dbadmin.sign_event SET sequence_num=(sequence_num + 1) WHERE ((priori			
1281	2796	34.619	0.008	Ack				
1282	2797	34.625	0.006	Cmd	INSERT INTO sign_event VALUES(45818,131585,0,768,230,2,1,1,0,"2001-03-30 08:49","0			
1287	2802	34.629	0.004	Ack				
1288	2804	34.638	0.009	Cmd	SELECT dbadmin.devctrlcfg.device_id FROM dbadmin.devctrlcfg WHERE (hwaddr = 1315			
1291	2807	34.641			One whole message for one sign transaction time is	14.242	Seconds	
1292	2808	34.641			Time on the one select statement	13.945	Seconds	
1293	2809	34.642			% Time in one select	98%		
1294	2810	34.642						
1295	2811	34.643			* 35 message signs =	490	Seconds	

cmsslow

Ready Sum=206.36

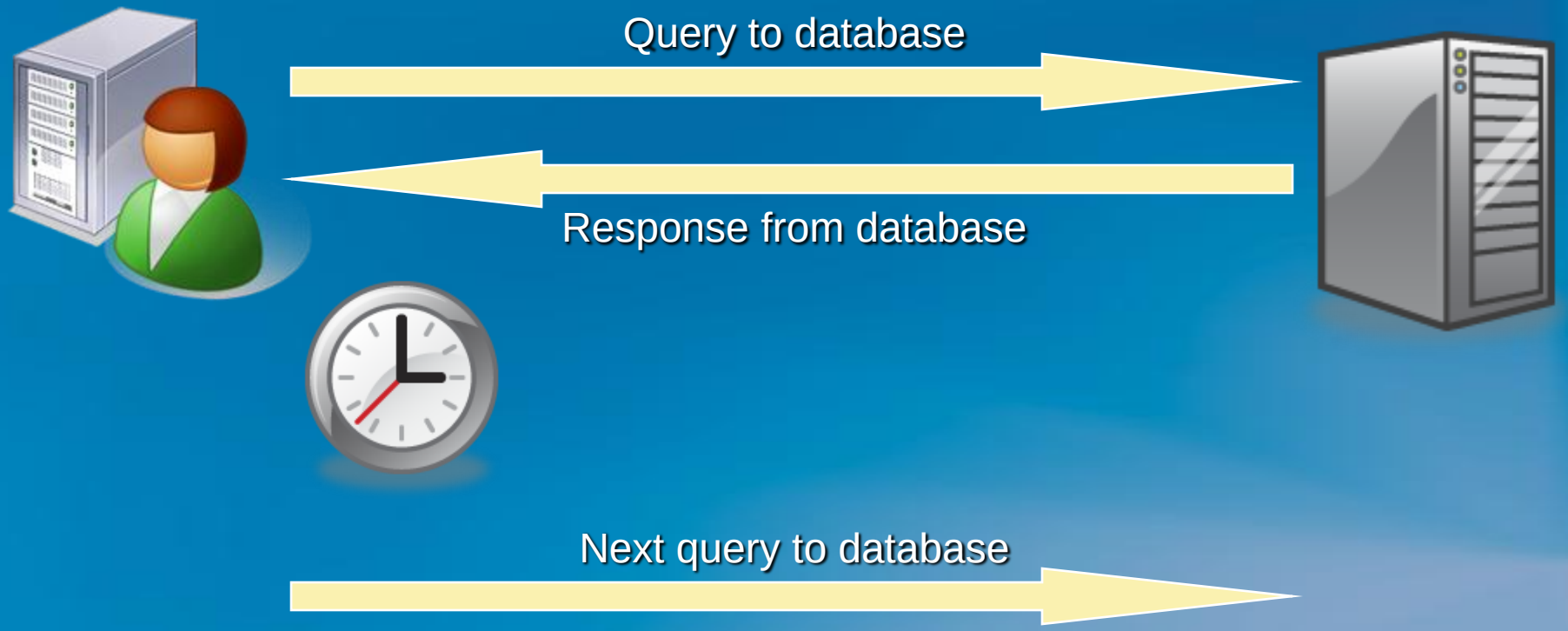
Observations…

- If a 10 Mb infrastructure was upgraded, it would hide this problem for a while, then stress the database, disks, network, and the problem would reappear

Microsoft

Observations…

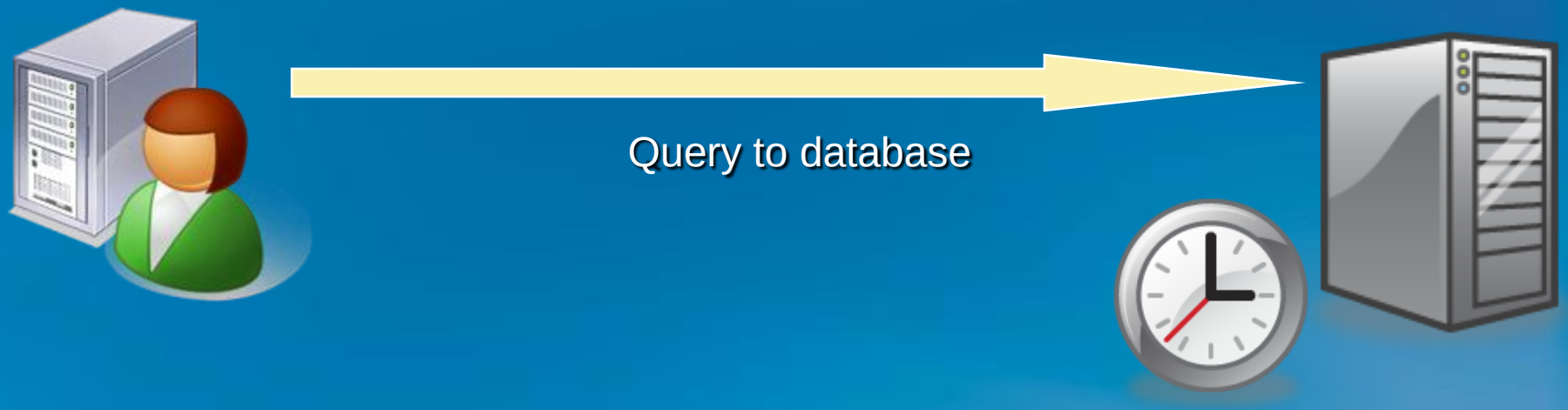
- If Visual Basic performance was a problem, Δt between “Query Response” and “Next Query” would be high



Microsoft

Observations…

- If database performance was a problem, Δt between “Query Sent” and “Query Response” would be high



Microsoft

Observations…

- If field communications were a problem, it would show up when we moved sniffer to field communications link

Microsoft

Demonstration Eight

demo

Slow FTP Issue

- First, a good FTP transfer

Microsoft

TCP Data Sequence Diagram (Transfer already in progress…)

Sender

Receiver

Packet #53 →

Microsoft

TCP Data Sequence Diagram (Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	

Microsoft

TCP Data Sequence Diagram
(Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	
Packet #55	→	

Microsoft

TCP Data Sequence Diagram
(Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	
Packet #55	→	
	←	Ack #53
Packet #56	→	

Microsoft

TCP Data Sequence Diagram
(Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	
Packet #55	→	
	←	Ack #53
Packet #56	→	
Packet #57	→	
Packet #58	→	
Packet #59	→	

Microsoft

TCP Data Sequence Diagram
(Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	
Packet #55	→	
	←	Ack #53
Packet #56	→	
Packet #57	→	
Packet #58	→	
Packet #59	→	
	←	Ack #58

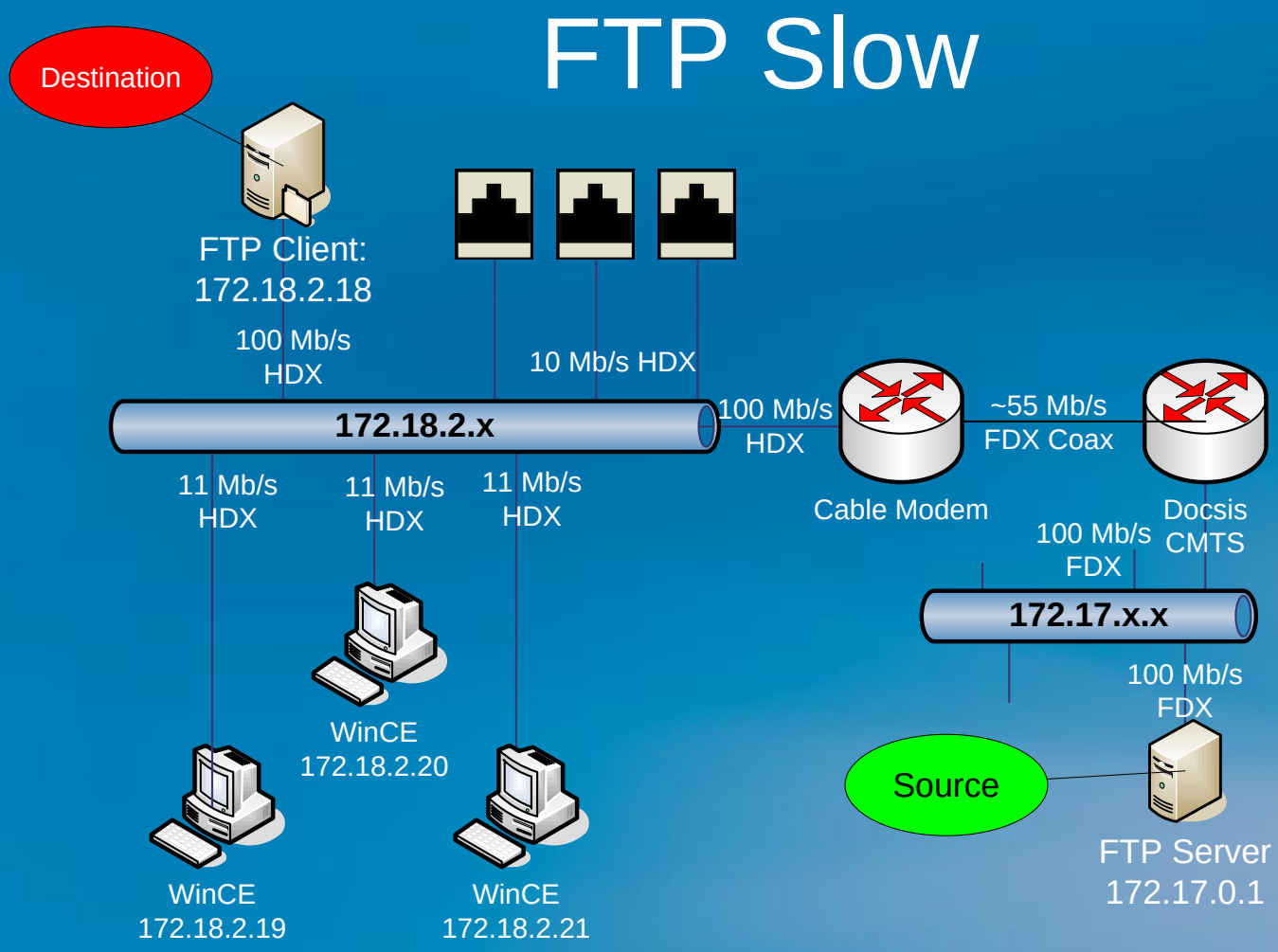
Microsoft

TCP Data Sequence Diagram
(Transfer already in progress…)

Sender		Receiver
Packet #53	→	
Packet #54	→	
Packet #55	→	
	←	Ack #53
Packet #56	→	
Packet #57	→	
Packet #58	→	
Packet #59	→	
	←	Ack #58
Packet #60	→	

Microsoft

Slow FTP Network Diagram



Microsoft

Demonstration Nine

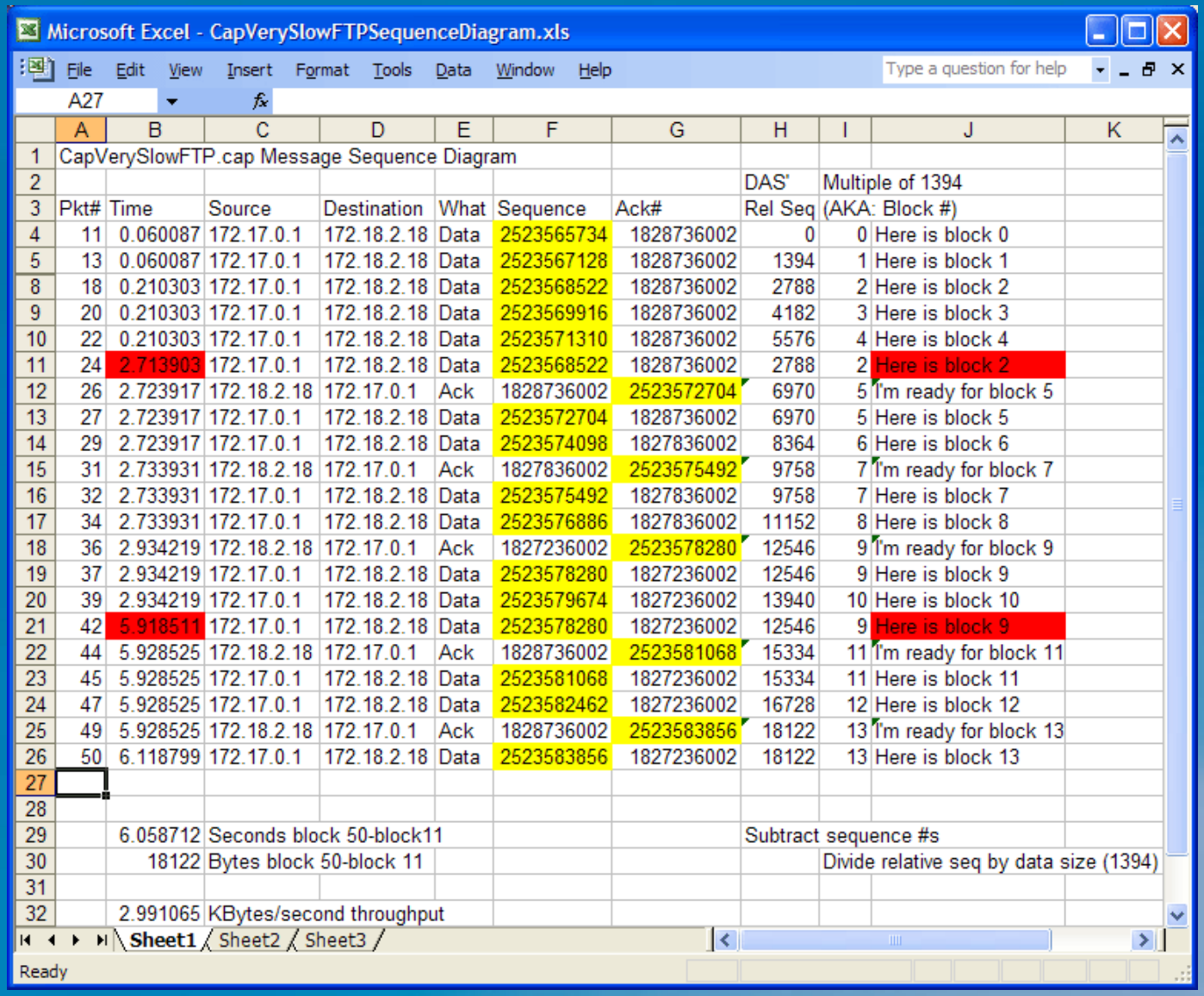
demo

Slow FTP Issue

- And a slow FTP transfer

Microsoft®

FTP Message Sequence


Microsoft Excel - CapVerySlowFTPSequenceDiagram.xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

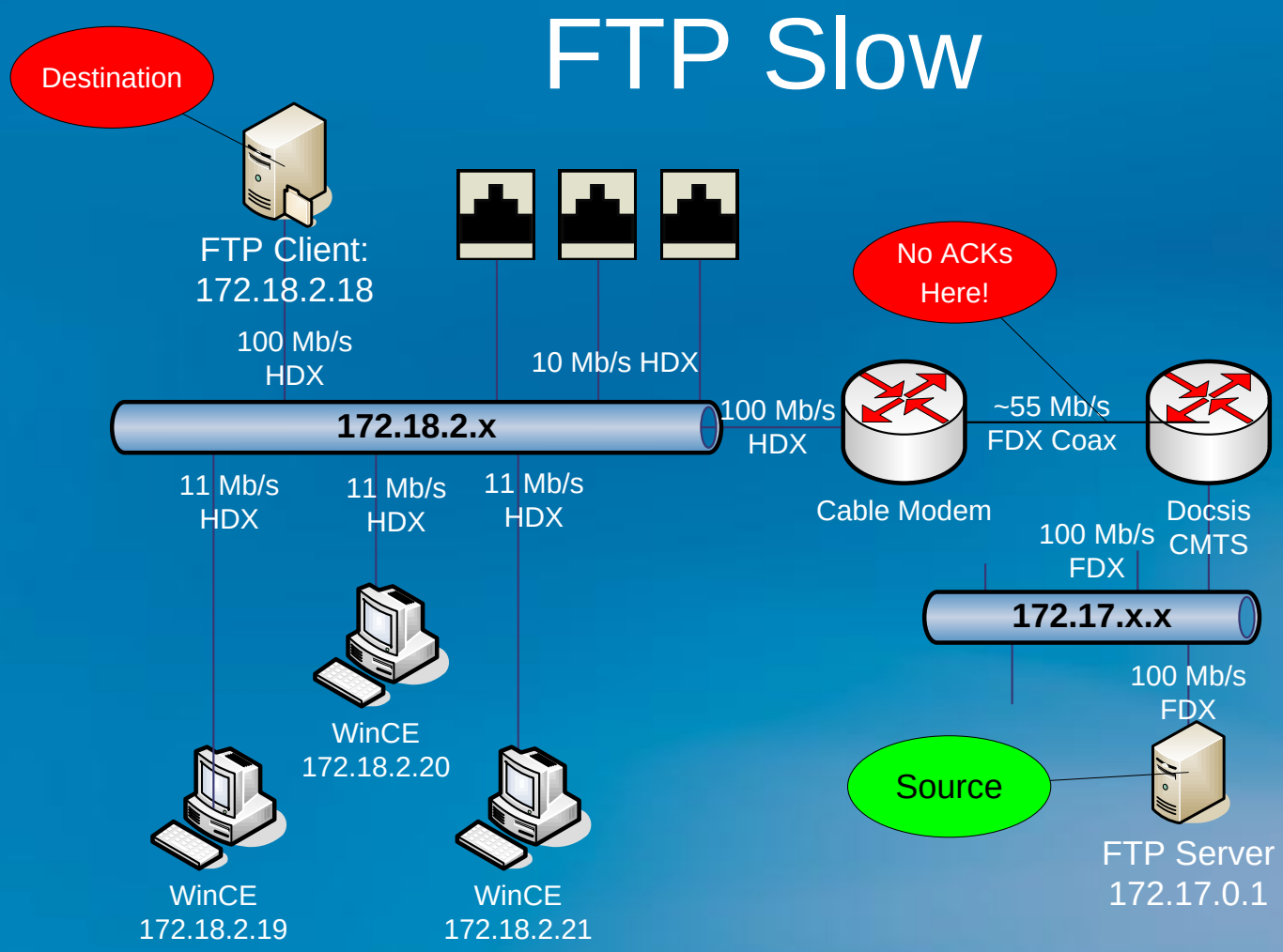
A27

	A	B	C	D	E	F	G	H	I	J	K
1	CapVerySlowFTP.cap Message Sequence Diagram										
2								DAS'	Multiple of 1394		
3	Pkt#	Time	Source	Destination	What	Sequence	Ack#	Rel Seq	(AKA: Block #)		
4	11	0.060087	172.17.0.1	172.18.2.18	Data	2523565734	1828736002	0	0	Here is block 0	
5	13	0.060087	172.17.0.1	172.18.2.18	Data	2523567128	1828736002	1394	1	Here is block 1	
8	18	0.210303	172.17.0.1	172.18.2.18	Data	2523568522	1828736002	2788	2	Here is block 2	
9	20	0.210303	172.17.0.1	172.18.2.18	Data	2523569916	1828736002	4182	3	Here is block 3	
10	22	0.210303	172.17.0.1	172.18.2.18	Data	2523571310	1828736002	5576	4	Here is block 4	
11	24	2.713903	172.17.0.1	172.18.2.18	Data	2523568522	1828736002	2788	2	Here is block 2	
12	26	2.723917	172.18.2.18	172.17.0.1	Ack	1828736002	2523572704	6970	5	I'm ready for block 5	
13	27	2.723917	172.17.0.1	172.18.2.18	Data	2523572704	1828736002	6970	5	Here is block 5	
14	29	2.723917	172.17.0.1	172.18.2.18	Data	2523574098	1827836002	8364	6	Here is block 6	
15	31	2.733931	172.18.2.18	172.17.0.1	Ack	1827836002	2523575492	9758	7	I'm ready for block 7	
16	32	2.733931	172.17.0.1	172.18.2.18	Data	2523575492	1827836002	9758	7	Here is block 7	
17	34	2.733931	172.17.0.1	172.18.2.18	Data	2523576886	1827836002	11152	8	Here is block 8	
18	36	2.934219	172.18.2.18	172.17.0.1	Ack	1827236002	2523578280	12546	9	I'm ready for block 9	
19	37	2.934219	172.17.0.1	172.18.2.18	Data	2523578280	1827236002	12546	9	Here is block 9	
20	39	2.934219	172.17.0.1	172.18.2.18	Data	2523579674	1827236002	13940	10	Here is block 10	
21	42	5.918511	172.17.0.1	172.18.2.18	Data	2523578280	1827236002	12546	9	Here is block 9	
22	44	5.928525	172.18.2.18	172.17.0.1	Ack	1828736002	2523581068	15334	11	I'm ready for block 11	
23	45	5.928525	172.17.0.1	172.18.2.18	Data	2523581068	1827236002	15334	11	Here is block 11	
24	47	5.928525	172.17.0.1	172.18.2.18	Data	2523582462	1827236002	16728	12	Here is block 12	
25	49	5.928525	172.18.2.18	172.17.0.1	Ack	1828736002	2523583856	18122	13	I'm ready for block 13	
26	50	6.118799	172.17.0.1	172.18.2.18	Data	2523583856	1827236002	18122	13	Here is block 13	
27											
28											
29		6.058712	Seconds block 50-block11					Subtract sequence #s			
30		18122	Bytes block 50-block 11						Divide relative seq by data size (1394)		
31											
32		2.991065	KBytes/second throughput								

Sheet1 Sheet2 Sheet3

Ready

Slow FTP Network Diagram

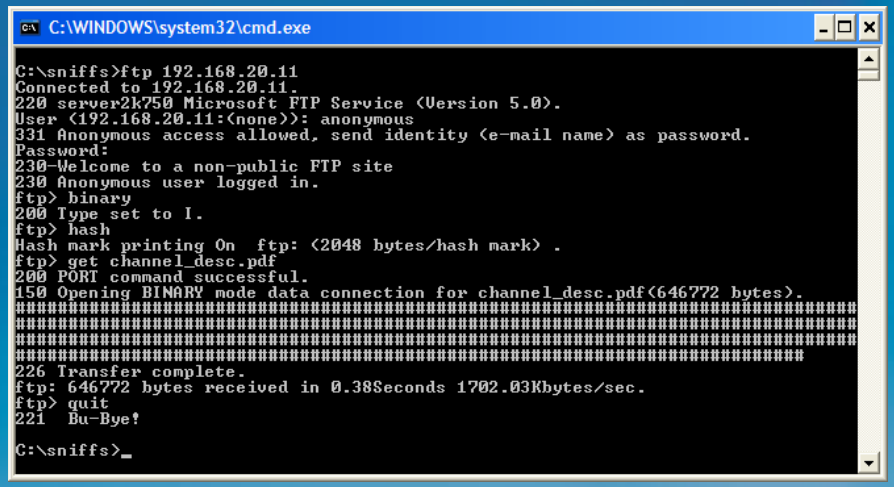


Microsoft

Demonstration Ten

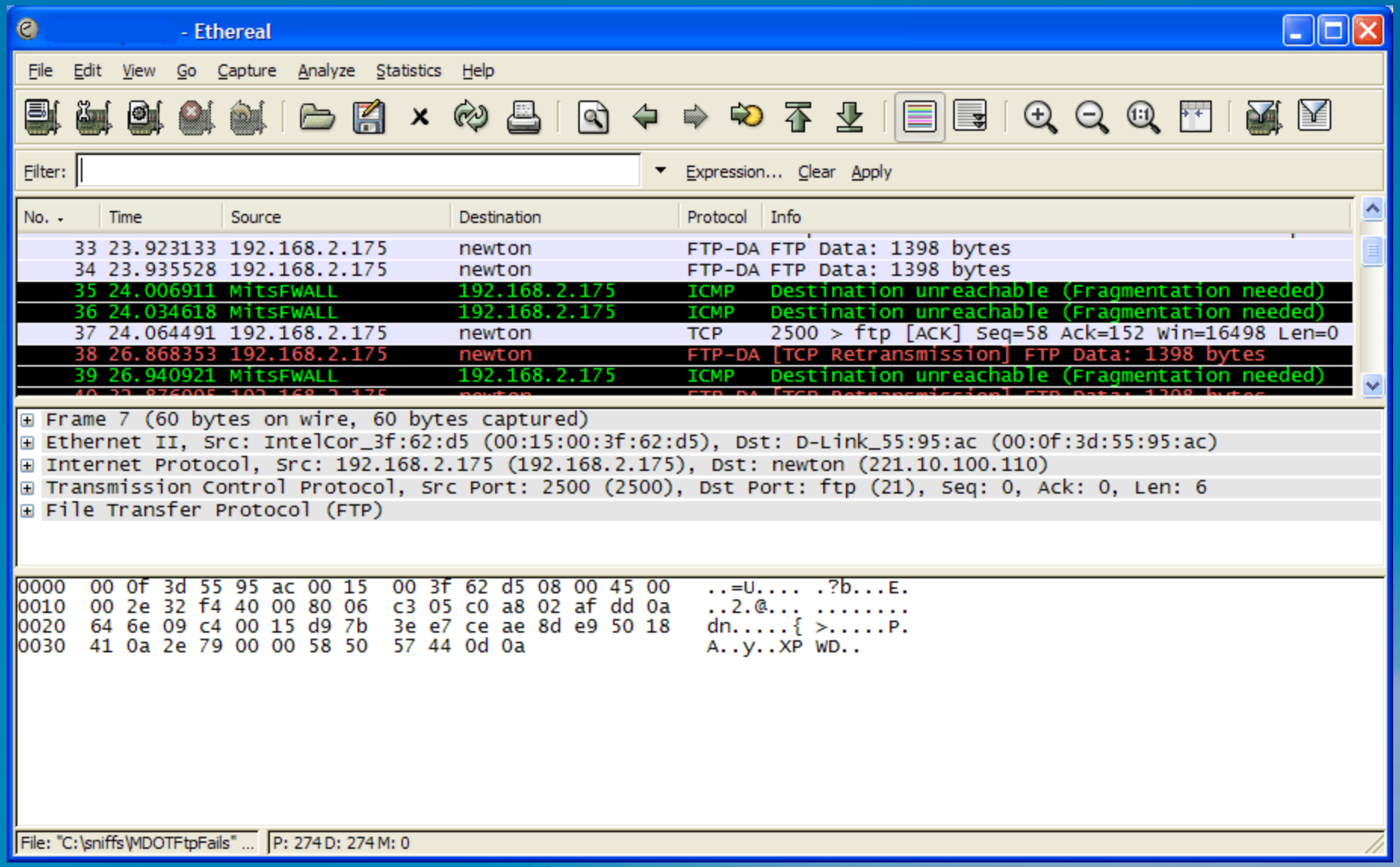
demo

FTP Fails Completely

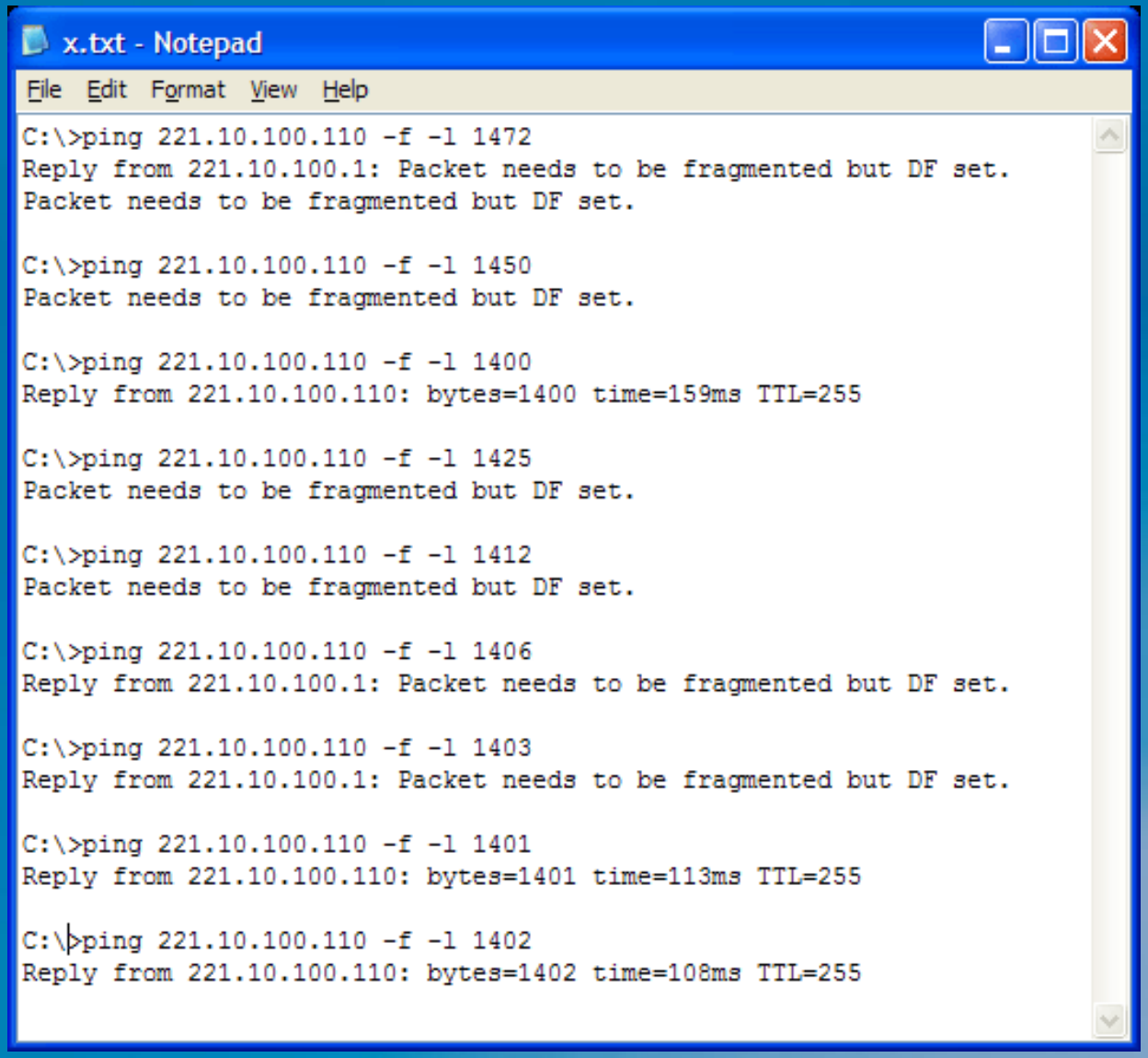


Microsoft®

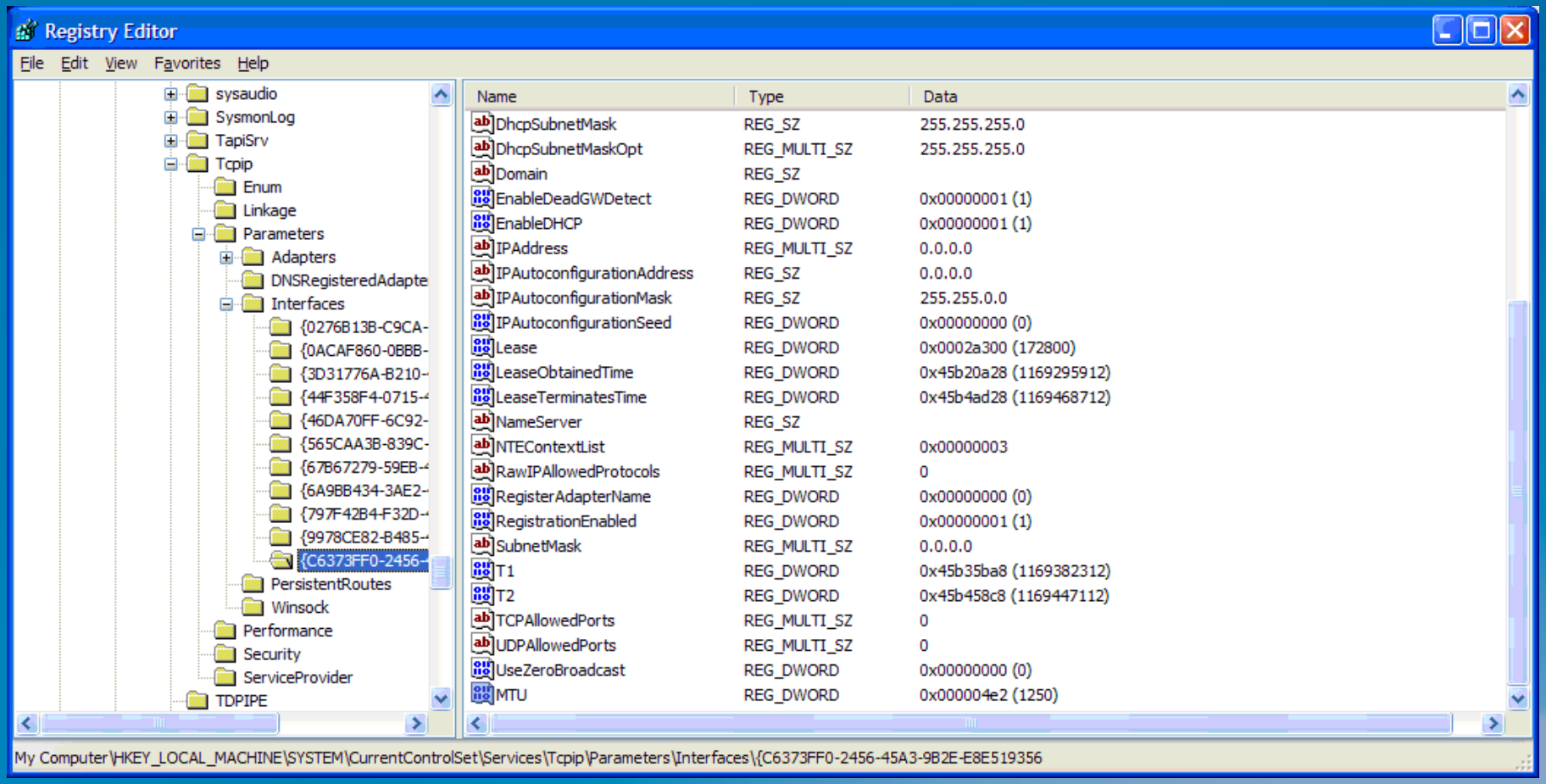
FTP Fails Completely



Fix #1: Find the MTU

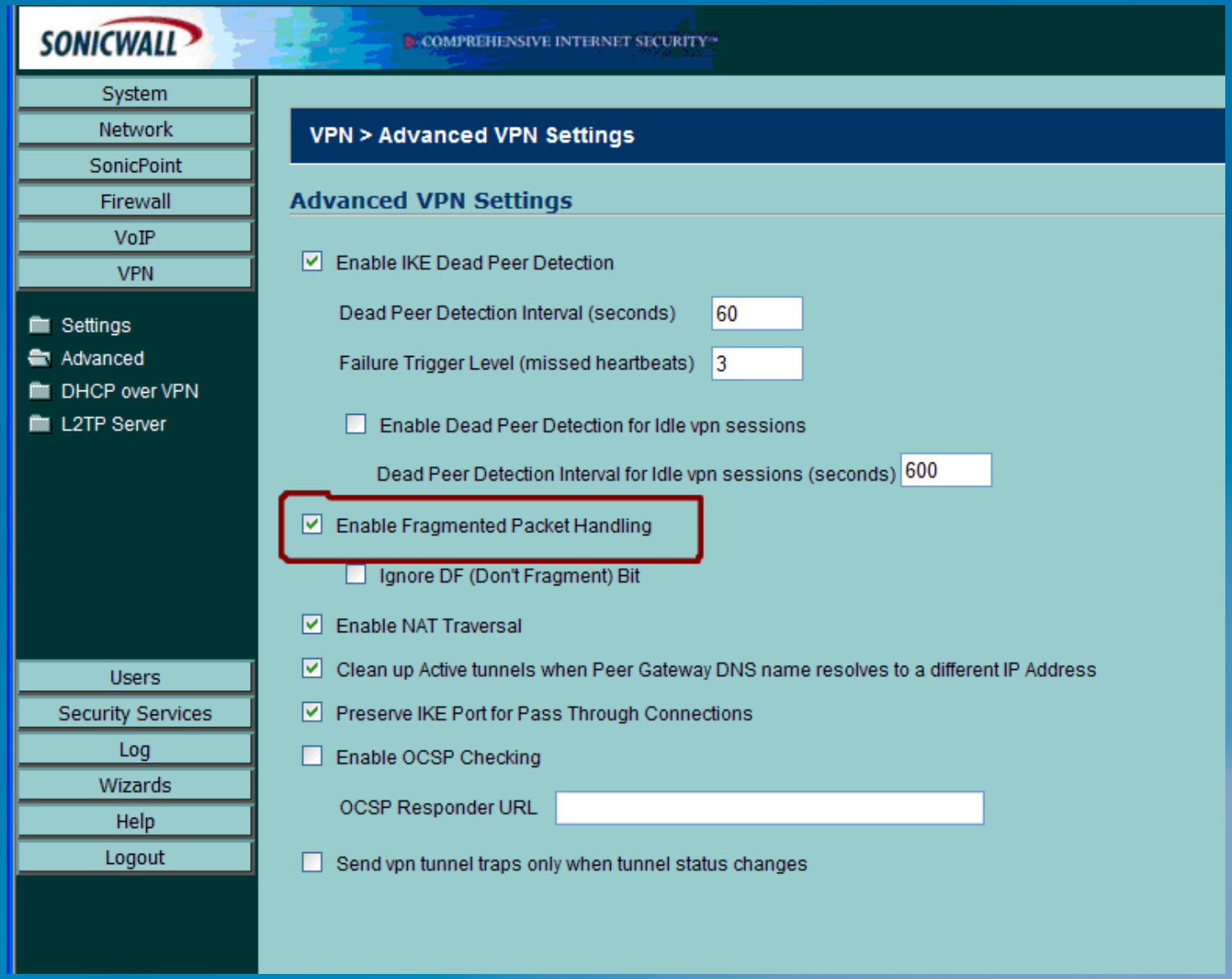


…Then Set Your Net Interface

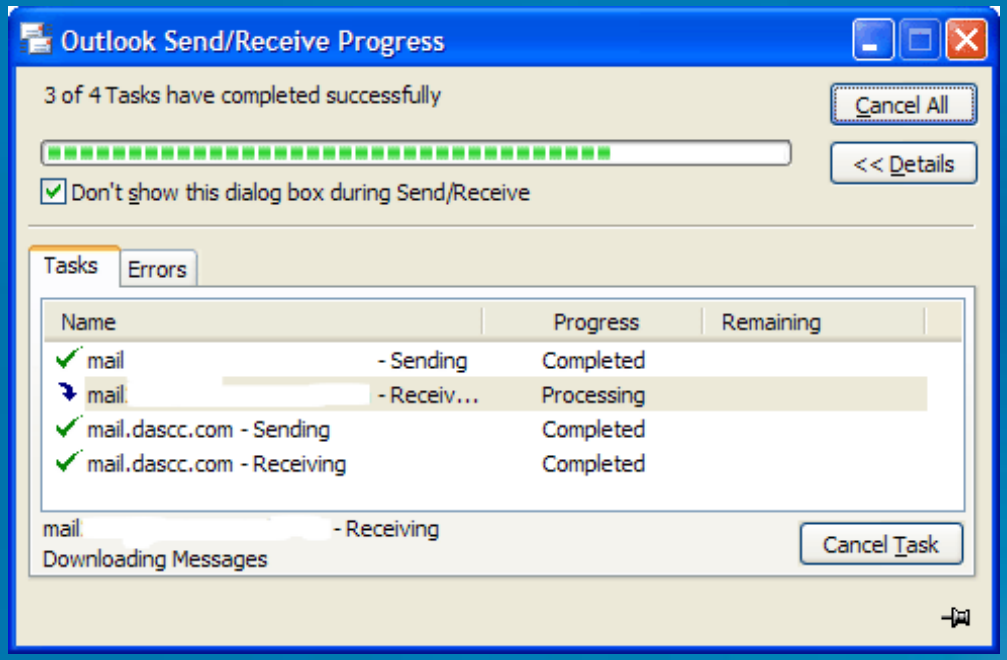


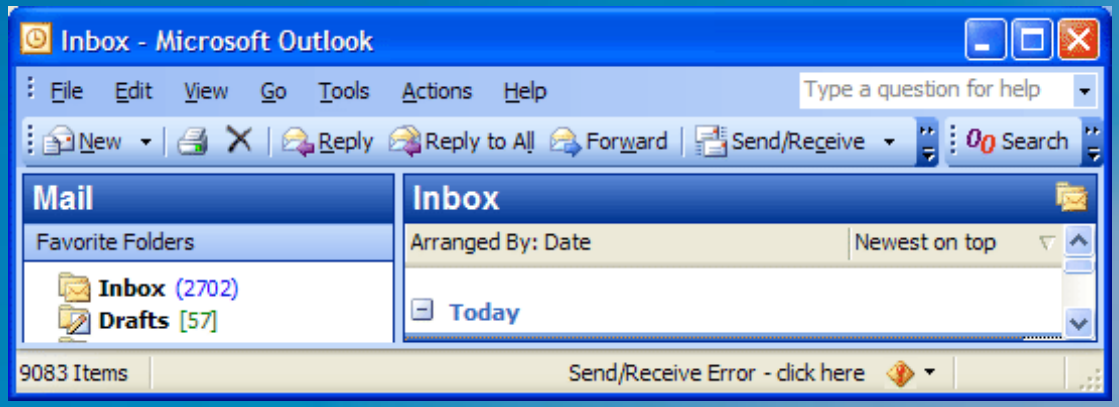
Microsoft

Fix #2: Allow Fragmentation



“My Mail Is Timing Out…”



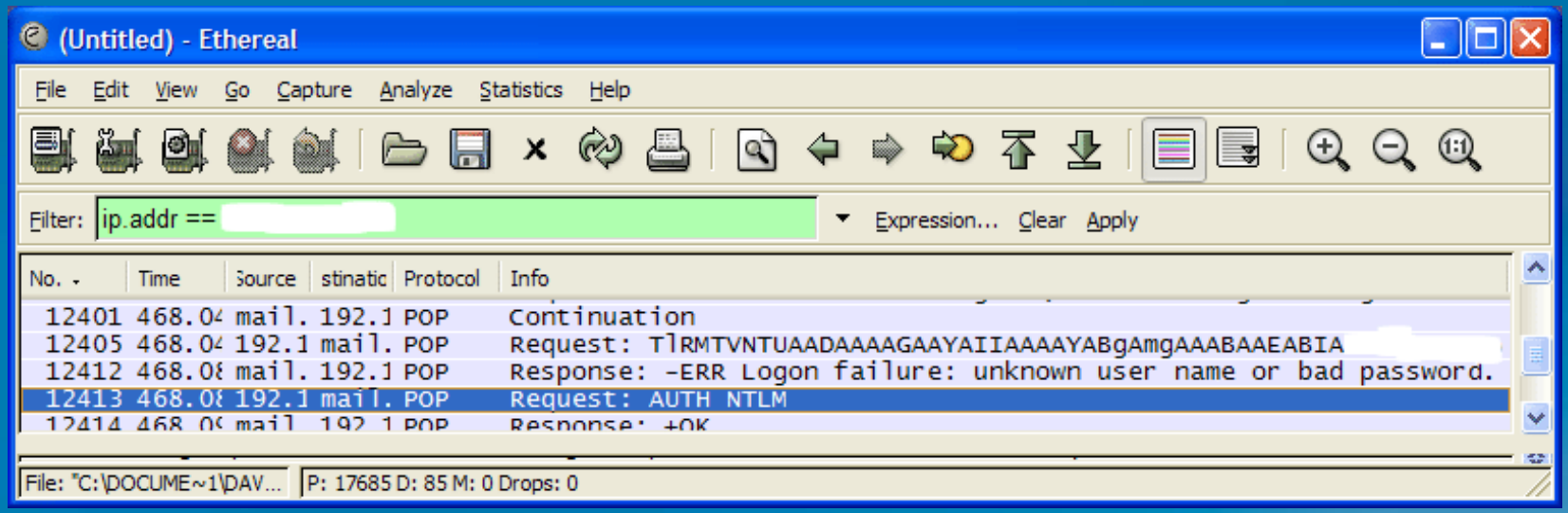


Microsoft

“My Mail Is Timing Out… Why?”

Microsoft

“My Mail Is Timing Out… Why?”



Microsoft

Quick Start Guide

- Install ethereal (I mean wireshark)
- Sniff while doing one thing (Web, file transfer, browse list, access Windows® SharePoint® Services, database…)
- Filter transfer to source and destination, or protocol type (DNS?)
- For delay situations, build a message sequence diagram
- Look and learn!

Microsoft®

WARNING! Not Everyone Is Happy When You Are Sniffing!

Appendix

Microsoft®

For More Information

- www.wireshark.org
- The Internet Engineering Task Force has all the RFCs at: http://ietf.org
- RFC 1180 - A TCP/IP Tutorial
- RFC 2821 - Simple Mail Transfer Protocol
- RFC 2045 - Multipurpose Internet Mail Extensions
- RFC 0793 - Transmission Control Protocol [TCP]
- *Internetworking with TCP/IP* by Douglas Comer (Prentice Hall, 2000)
- The Cable Guy – July 2004: Path Maximum Transmission Unit (PMTU) Black Hole Routers at:
  - www.microsoft.com/technet/community/columns/cableguy/cg0704.mspx
- Questions? Comments? I'd love to hear from you! webcast@dascc.com

Microsoft

For More Information

- This solution
  - Contact David Soussan at:
    - webcast@dascc.com
- Microsoft solutions and products:
  - Contact your Microsoft representative
  - Visit: www.microsoft.com

Microsoft

Questions and Answers

- Submit text questions using the “Ask” button.
- Don’t forget to fill out the survey.
- For upcoming and previously live webcasts: **www.microsoft.com/webcasts**
- Got webcast content ideas? Contact us at: **http://go.microsoft.com/fwlink/?LinkId=41781**
- Today's webcast was presented using Microsoft® Office Live Meeting. Get a free 14-day trial by visiting: **www.microsoft.com/presentlive**

Microsoft Office Live Meeting

Microsoft®