

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

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!”

Prerequisites

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

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

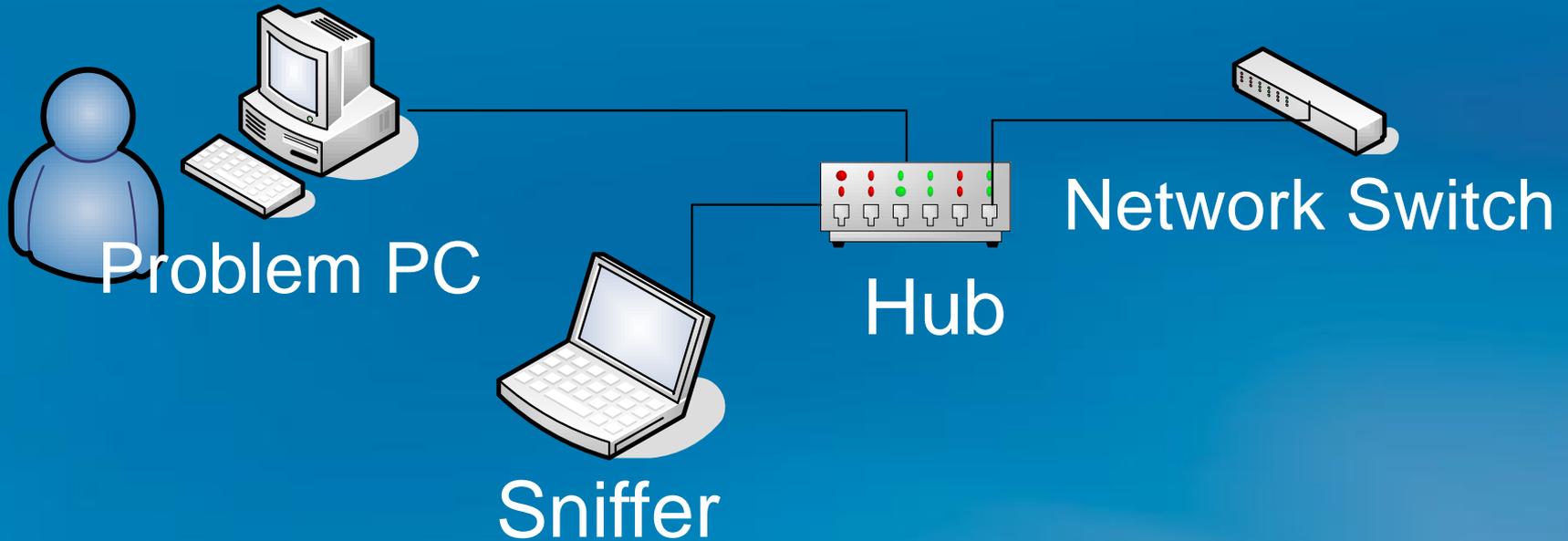
Sniffing?



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

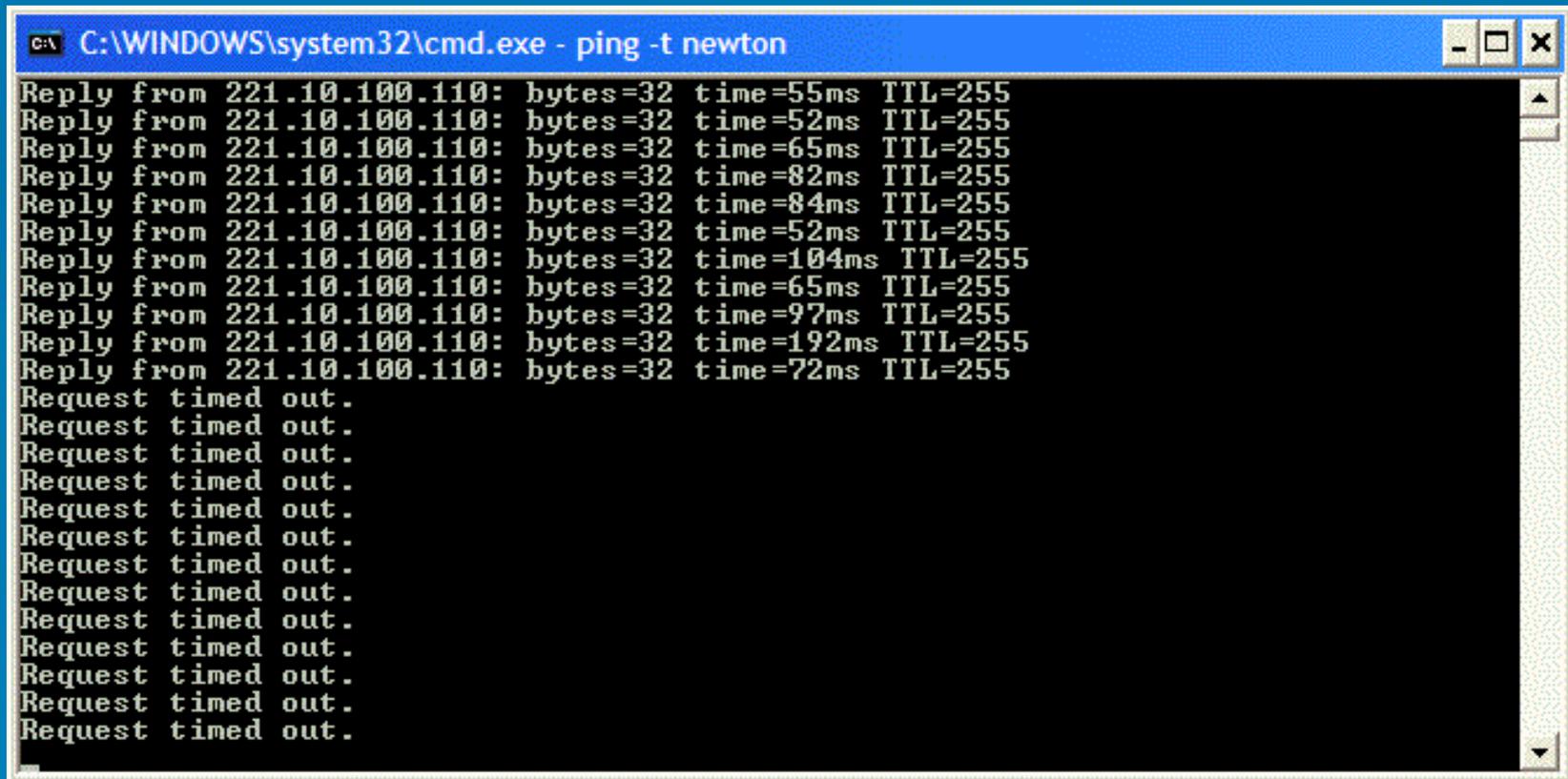
Ethereal (Now Wireshark)

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

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

Scenario One



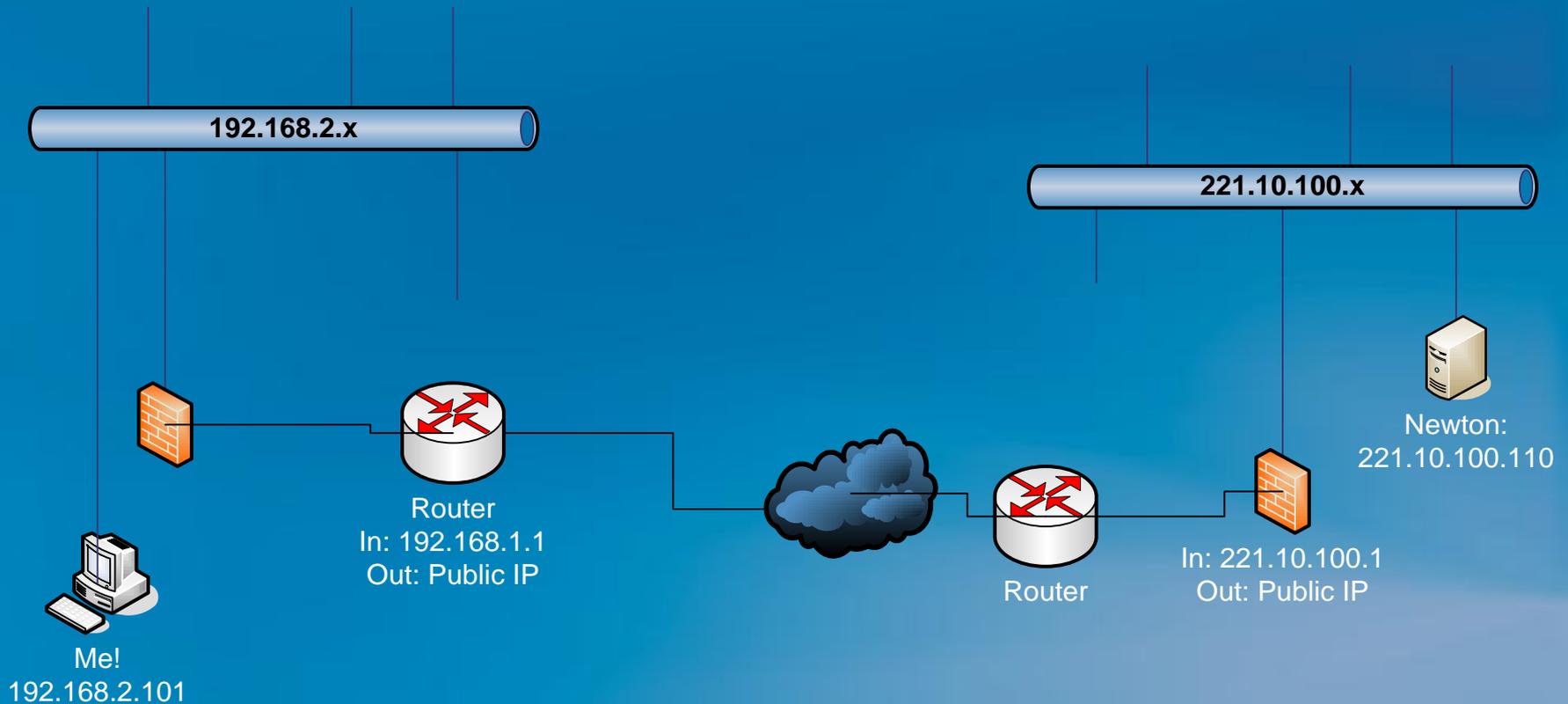
A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe - ping -t newton". The window displays the output of a continuous ping command to the IP address 221.10.100.110. The first 10 replies are successful, showing varying response times (e.g., 55ms, 52ms, 65ms, 82ms, 84ms, 52ms, 104ms, 65ms, 97ms, 192ms) and a TTL of 255. Following these, 10 consecutive "Request timed out." messages are displayed, indicating a complete loss of connectivity.

```
C:\WINDOWS\system32\cmd.exe - ping -t newton
Reply from 221.10.100.110: bytes=32 time=55ms TTL=255
Reply from 221.10.100.110: bytes=32 time=52ms TTL=255
Reply from 221.10.100.110: bytes=32 time=65ms TTL=255
Reply from 221.10.100.110: bytes=32 time=82ms TTL=255
Reply from 221.10.100.110: bytes=32 time=84ms TTL=255
Reply from 221.10.100.110: bytes=32 time=52ms TTL=255
Reply from 221.10.100.110: bytes=32 time=104ms TTL=255
Reply from 221.10.100.110: bytes=32 time=65ms TTL=255
Reply from 221.10.100.110: bytes=32 time=97ms TTL=255
Reply from 221.10.100.110: bytes=32 time=192ms TTL=255
Reply from 221.10.100.110: bytes=32 time=72ms TTL=255
Request timed out.
```

Intermittent Network Connectivity One

A Troubled Network

Intermittent Internet Connectivity



Demonstration One

demo

Intermittent Internet One

The actual data sniff in Ethereal!

Microsoft[®]

Finding the Mystery Router

The screenshot displays two instances of the Wireshark network protocol analyzer. The top instance shows a capture filter set to 'icmp' and a list of captured packets. The bottom instance shows a detailed view of a selected packet, including the Ethernet II, Internet Protocol, and Internet Control Message Protocol layers, along with a hex dump and ASCII representation.

Top Window: CapIntermittentNetwork1 - Ethereal

Filter: icmp

No.	Time	Source	Destination	Protocol	Info
14715	11:17:00.997259	newton	192.168.123.108	ICMP	Echo (ping) reply
14721	11:17:01.990130	192.168.123.108	newton	ICMP	Echo (ping) request
14722	11:17:01.990148	newton	192.168.123.108	ICMP	Echo (ping) reply
14728	11:17:02.992085	192.168.123.108	newton	ICMP	Echo (ping) request
14731	11:17:02.992829	newton	192.168.123.108	ICMP	Echo (ping) reply

Bottom Window: Detailed View

Ethernet II, Src: newton (08:00:20:8f:cd:5e), Dst: MitsFWALL (00:06:b1:09:92:fc)
Destination: MitsFWALL (00:06:b1:09:92:fc)
Source: newton (08:00:20:8f:cd:5e)
Type: IP (0x0800)

Internet Protocol, Src: newton (221.10.100.110), Dst: 192.168.123.108 (192.168.123.108)

Internet Control Message Protocol

```
0000 00 06 b1 09 92 fc 08 00 20 8f cd 5e 08 00 45 00  ....].. ..^..E.  
0010 00 3c 94 1e 40 00 ff 01 6a 14 dd 0a 64 6e c0 a8  <..@... j...dn..  
0020 7b 6c 00 00 5a 2c 02 00 f9 2f 61 62 63 64 65 66  {l..Z... ./abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
```

Destination Hardware Addr... P: 20000 D: 580 M: 0

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    1e0
221.10.101.0          atms1                 U        2   9838    1e1
224.0.0.0             copernicus            U        3      0    1e0
default               p50mitsc             UG      0     589
default               221.10.100.202      UG      0     507
default               MitsFWALL            UG      0      23
```

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?

TRENDnet
TRENDware, USA
What's Next in Networking

MIMO TECHNOLOGY 108g
EXTENDED RANGE

8x MIMO MEMORY 800%
108g XR

108Mbps 802.11g Wireless MIMO Router TEW-611BRP

BASIC ADVANCED TOOLS STATUS HELP

BASIC

- WIZARD
- WAN
- LAN
- DHCP
- WIRELESS

LAN

Network Settings

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN SETTINGS

IP Address :

Default Subnet Mask :

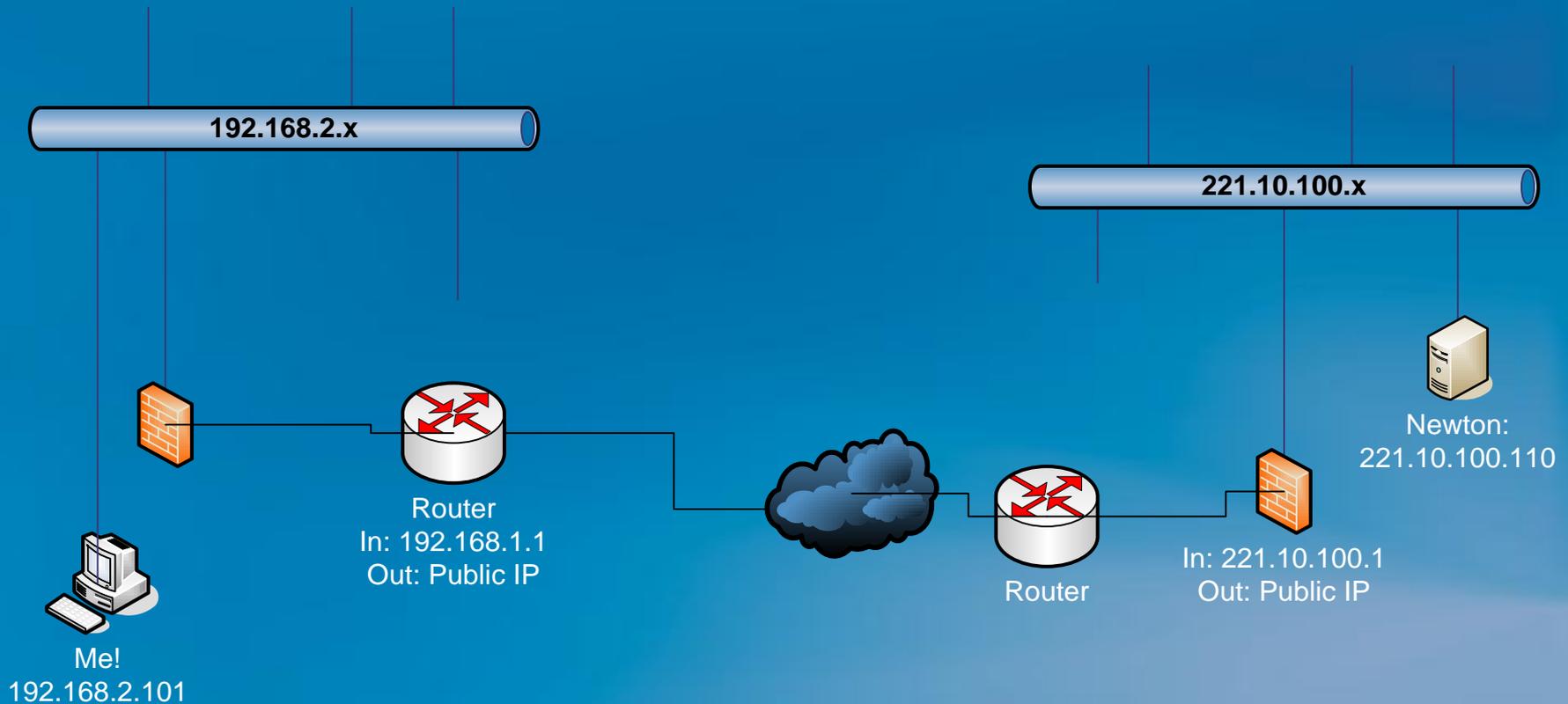
RIP SETTINGS

RIP Announcement :

Router Metric :

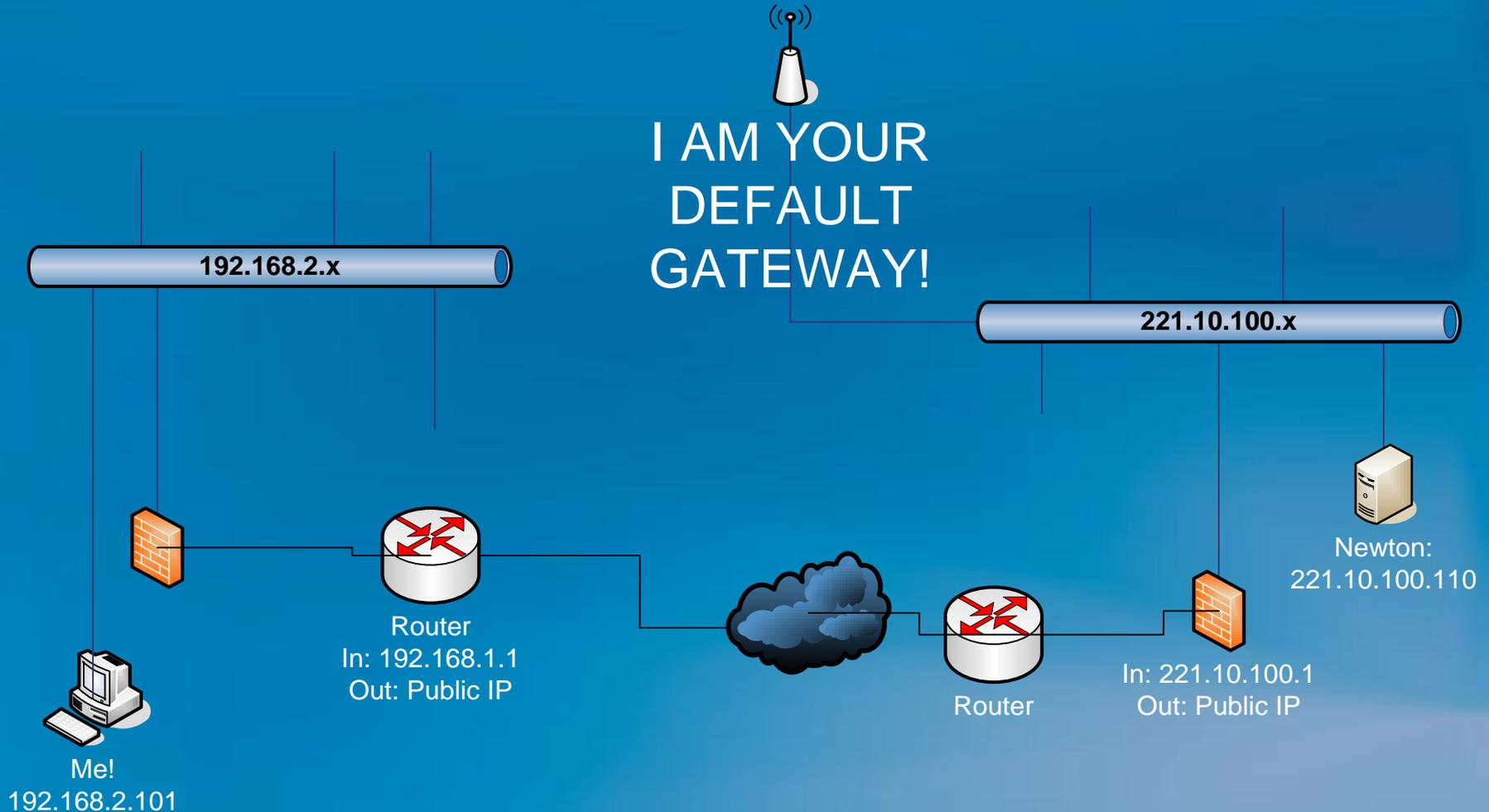
Network: Before

Intermittent Internet Connectivity



Network: After (Broken)

Intermittent Internet Connectivity



Demonstration Two

demo

Intermittent Internet Two

Exact same symptom, different root cause

Microsoft[®]

Intermittent Internet Two

The screenshot shows the Wireshark interface with a network traffic capture. The main display area shows a list of captured packets. Packet 34 is selected, showing its details and raw data.

No.	Time	Source	Destination	Protocol	Info
33	21.084232	Dell_b2:a7:0d	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.165
34	21.084271	192.168.1.1	Dell_b2:a7:0d	ARP	192.168.1.1 is at 00:0f:cc:17:9c:a8
35	21.084326	Adtran_0a:b6:5d	Dell_b2:a7:0d	ARP	192.168.1.1 is at 00:a0:c8:0a:b6:5d
36	21.084412	192.168.1.165	209.191.93.52	ICMP	Echo (ping) request
37	21.084661	192.168.1.1	192.168.1.165	ICMP	Destination unreachable (Host unreachable)

Frame 34 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 192.168.1.1 (00:0f:cc:17:9c:a8), Dst: Dell_b2:a7:0d (00:12:3f:b2:a7:0d)
Destination: Dell_b2:a7:0d (00:12:3f:b2:a7:0d)
Source: 192.168.1.1 (00:0f:cc:17:9c:a8)
Type: ARP (0x0806)
Trailer: 00

```
0000 00 12 3f b2 a7 0d 00 0f cc 17 9c a8 08 06 00 01 ..?.....  
0010 08 00 06 04 00 02 00 0f cc 17 9c a8 c0 a8 01 01 .....  
0020 00 12 3f b2 a7 0d c0 a8 01 a5 00 00 00 00 00 00 ..?.....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
```

File: "C:\sniffs\CapIntermitte... | P: 1254 D: 1254 M: 0

Demonstration Three

demo

“How can she possibly know everything I’m doing????”

Microsoft[®]

Filtered on DNS Queries

The screenshot shows the Wireshark interface with the filter 'dns' applied. The packet list pane shows several DNS packets, with packet 3601 selected. The packet details pane shows the structure of a DNS query for 'www.v19170dc0-7597-11d.com'. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Info
2382	23:10:33.224	ns.tds.net	192.168.9.104	DNS	Standard query response PTR ipt-ucca19.01at.adf.v
3544	23:14:15.939	192.168.9.104	ns.tds.net	DNS	Standard query A liveupdate.symantecliveupdate.co
3545	23:14:15.962	ns.tds.net	192.168.9.104	DNS	Standard query response CNAME liveupdate.symantec
3600	23:14:34.403	192.168.9.104	ns.tds.net	DNS	Standard query A www.v19170dc0-7597-11d.com
3601	23:14:34.673	ns.tds.net	192.168.9.104	DNS	Standard query response CNAME v19170dc0-7597-11d.
4822	23:16:37.671	192.168.9.104	ns.tds.net	DNS	Standard query A www.natplan.com
4823	23:16:38.007	ns.tds.net	192.168.9.104	DNS	Standard query response A 12.148.227.230
5004	23:17:01.138	192.168.9.104	ns.tds.net	DNS	Standard query A extconn1.jacksonnational.com

Queries

- www.v19170dc0-7597-11d.com: type A, class IN

Answers

- www.v19170dc0-7597-11d.com: type CNAME, class IN, cname v19170dc0-7597-11d.com
- v19170dc0-7597-11d.com: type A, class IN, addr 64.49.213.137

Authoritative nameservers

- v19170dc0-7597-11d.com: type NS, class IN, ns ns.rackspace.com
- v19170dc0-7597-11d.com: type NS, class IN, ns ns2.rackspace.com

Packet Bytes

```
0000  00 0b db 04 2f 87 00 06 25 e3 19 51 08 00 45 00  ....//...%..Q..E.  
0010  00 b3 de a3 40 00 3d 11 c6 7b cc f6 01 14 c0 a8  ....@.=. .{.....  
0020  09 68 00 35 0b c4 00 9f 8b 50 00 06 81 80 00 01  .h.5.... .P.....  
0030  00 02 00 02 00 02 03 77 77 77 12 76 31 39 31 37  .....w ww.v1917  
0040  30 64 63 30 2d 37 35 39 37 2d 31 31 64 03 63 6f  0dc0-759 7-11d.co  
0050  6d 00 00 01 00 01 c0 0c 00 05 00 01 00 00 01 2c  m.....  
0060  00 02 c0 10 c0 10 00 01 00 01 00 00 01 2c 00 04  .....  
0070  40 31 d5 89 c0 10 00 02 00 01 00 00 01 2c 00 0f  @1.....  
0080  02 6e 73 09 72 61 63 6b 73 70 61 63 65 c0 23 c0  .ns.rack space.#.  
0090  10 00 02 00 01 00 00 01 2c 00 06 03 6e 73 32 c0  ..... .ns2.  
00a0  59 c0 56 00 01 00 01 00 01 14 d1 00 04 cf eb 10  Y.V.....  
00b0  02 c0 71 00 01 00 01 00 01 30 72 00 04 cf 47 2c  ..q..... .Or...G,  
00c0  79 y
```

P: 12278 D: 190 M: 0

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?

Spector and eBlaster Spy Software - Internet Monitoring Software - Micros...

File Edit View Favorites Tools Help

Address <http://spectorsoft.com/> Go Links >>

SPECTORSOFT
An Inc. 500 Company

Home Products Press Purchase About

Automatically Record Everything They Do

FOR HOME & SMALL BUSINESS

Spector Pro **NEW!**
Powerful Monitoring, Extreme Ease of Use

Records Every Exact Detail of their PC and Internet Activity.

PC Magazine Editors' Choice

Spector Pro combines powerful monitoring features with extreme ease of use, making it the ideal choice for home users and small businesses. Records emails, chats, IMs, keystrokes, web sites, plus provides screen snapshots, internet blocking and danger alerts.

[MORE INFO](#) [BUY NOW](#)

eBlaster **UPDATED!**
Remote Monitoring Software

Knowing **EVERYTHING** They Do Online is as Easy as Checking Your Email.

Install eBlaster on the computer you wish to monitor and start receiving copies of every email sent and received on that PC.

-- PLUS --

Receive complete transcripts of all chat conversations and instant messages that take place on the monitored PC. **All sent to YOUR Email address.**

Remote Monitoring

[MORE INFO](#) [BUY NOW](#)

FOR C...
Sp...
Recc...
Emp...
Sp...
Know...
Onlin...

Done Internet

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

Filter: ip.addr == 10.10.10.103

No.	Time	Source	Destination	Protocol	Info
190	17:05:37.844300	10.10.10.103	10.10.10.255	NBNS	Registration NB USCEX<00>
191	17:05:37.795774	10.10.10.103	10.10.10.255	NBNS	Registration NB USCEX<00>
192	17:05:38.546709	10.10.10.103	10.10.10.255	NBNS	Registration NB USCEX<00>
193	17:05:39.638432	10.10.10.103	10.10.10.1	DNS	Standard query SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.uscex.local
194	17:05:39.638539	10.10.10.103	10.10.10.1	DNS	Standard query response, No such name
195	17:05:39.650320	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
196	17:05:39.651343	10.10.10.103	10.10.10.1	DNS	Standard query response, No such name
197	17:05:39.652935	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
198	17:05:39.653564	10.10.10.103	10.10.10.1	DNS	Standard query response, No such name
199	17:05:39.661911	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
200	17:05:39.662971	10.10.10.103	10.10.10.1	DNS	Standard query response, No such name
201	17:05:39.664118	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
202	17:05:39.665085	10.10.10.103	10.10.10.1	DNS	Standard query response, No such name
203	17:05:39.674313	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
204	17:05:39.675345	10.10.10.103	10.10.10.255	NBNS	Name query NB USCEX<1c>
205	17:05:39.675772	10.10.10.200	10.10.10.103	NBNS	Name query response NB 10.10.10.200
206	17:05:39.676509	10.10.10.103	10.10.10.255	SMB_NE	SAM LOGON request from client
209	17:05:39.677367	10.10.10.103	10.10.10.200	SMB_NE	SAM LOGON request from client
210	17:05:39.677831	10.10.10.200	10.10.10.103	SMB_NE	SAM Active Directory Response - user unknown
211	17:05:39.678224	10.10.10.1	10.10.10.103	DNS	Standard query response, No such name
212	17:05:39.679659	10.10.10.103	10.10.10.255	SMB_NE	SAM LOGON request from client
213	17:05:39.680049	10.10.10.103	10.10.10.200	SMB_NE	SAM LOGON request from client

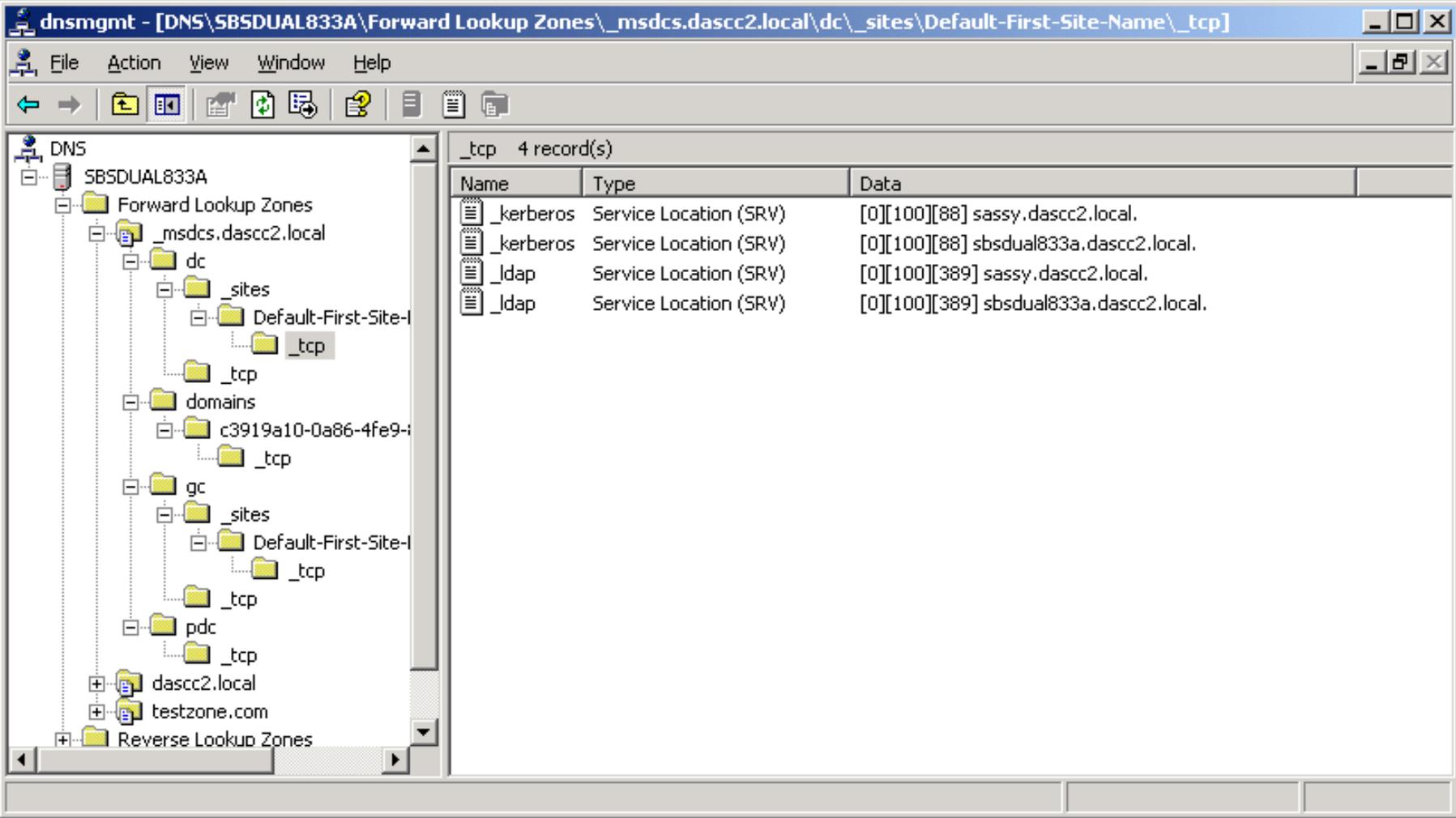
Frame 193 (123 bytes on wire, 123 bytes captured)
Ethernet II, Src: DellComp_50:5b:96 (00:06:5b:50:5b:96), Dst: 10.10.10.1 (00:00:89:29:0d:84)
Internet Protocol, Src: 10.10.10.103 (10.10.10.103), Dst: 10.10.10.1 (10.10.10.1)
User Datagram Protocol, Src Port: 1026 (1026), Dst Port: domain (53)
Domain Name System (query)

```
0000  00 00 89 29 0d 84 00 06 5b 50 5b 96 08 00 45 00  ...)... [P[...E.  
0010  00 6d 00 0c 00 00 40 11 51 f9 0a 0a 0a 67 0a 0a  .m....@. Q....g..  
0020  0a 01 04 02 00 35 00 59 a7 9d 50 4a 01 00 00 01  ....5.Y ..PJ....  
0030  00 00 00 00 00 00 05 5f 6c 64 61 70 04 5f 74 63  ....._ldap._tc  
0040  70 17 44 65 66 61 75 6c 74 2d 46 69 72 73 74 2d  p.Default t-First-  
0050  53 69 74 65 2d 4e 61 6d 65 06 5f 73 69 74 65 73  Site-Nam e._sites  
0060  02 64 63 06 5f 6d 73 64 63 73 05 75 73 63 65 78  .dc._msd cs.uscex  
0070  05 6c 6f 63 61 6c 00 00 21 00 01  .local.. !..
```

File: "C:\uscex\RandyLoginInAndOutSe... |P: 66672 D: 65667 M: 0

* Active Directory® directory service

What DNS Should Look Like



The screenshot shows the DNS Management console for the server SBSDual833A. The left pane displays a tree view of the DNS hierarchy, including Forward Lookup Zones and Reverse Lookup Zones. The right pane shows the configuration for the _tcp zone, displaying 4 records.

Name	Type	Data
_kerberos	Service Location (SRV)	[0][100][88] sassy.dascc2.local.
_kerberos	Service Location (SRV)	[0][100][88] sbsdual833a.dascc2.local.
_ldap	Service Location (SRV)	[0][100][389] sassy.dascc2.local.
_ldap	Service Location (SRV)	[0][100][389] sbsdual833a.dascc2.local.

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

SysAt167SpywareInfected - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.1.112 and ip.addr eq 217.160.230.10) and (t... Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
26	15:56:39.979484	mx00.1and1.com	192.168.1.112	SMTP	Response: 250 <sruli@wits.
27	15:56:39.979895	192.168.1.112	mx00.1and1.com	SMTP	Command: DATA
29	15:56:40.052864	mx00.1and1.com	192.168.1.112	TCP	smtp > 3770 [ACK] Seq=178
30	15:56:40.055439	mx00.1and1.com	192.168.1.112	SMTP	Response: 354 Enter mail,
31	15:56:40.056130	192.168.1.112	mx00.1and1.com	SMTP	Message Body
32	15:56:40.056308	192.168.1.112	mx00.1and1.com	SMTP	Message Body
33	15:56:40.056356	192.168.1.112	mx00.1and1.com	SMTP	Message Body
34	15:56:40.056482	192.168.1.112	mx00.1and1.com	SMTP	Message Body
35	15:56:40.056531	192.168.1.112	mx00.1and1.com	SMTP	Message Body

Transmission Control Protocol, Src Port: 3770 (3770), Dst Port: smtp (25), Seq: 89, ACK

Simple Mail Transfer Protocol

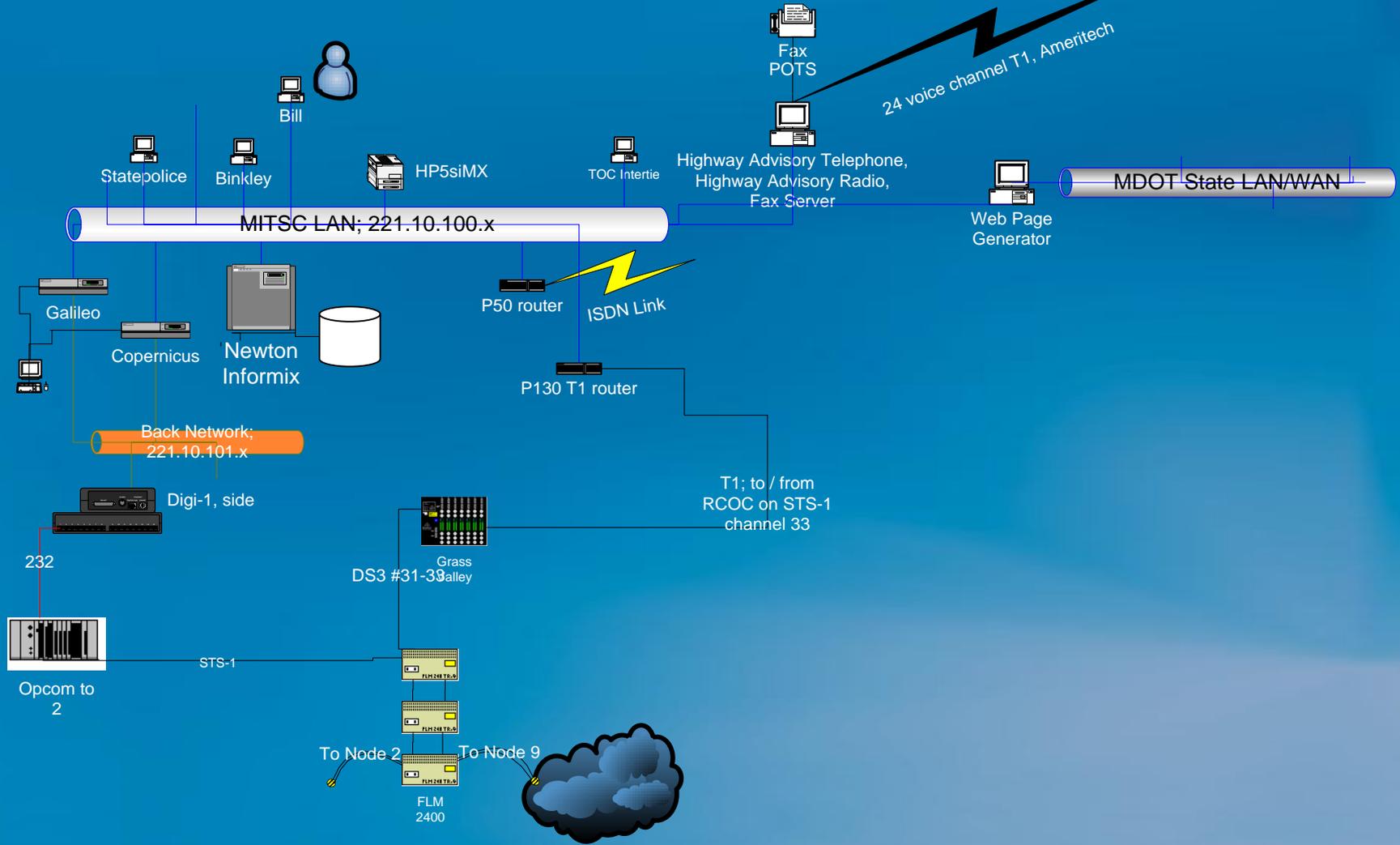
Message: Date: Thu, 22 Dec 2005 15:56:53 -0500\r\n
Message: To: "sruli" <sruli@wits.ca>\r\n
Message: From: "sruli" <sruli@tirana.gov.al>\r\n
Message: Subject: Danyell\r\n
Message: Message-ID: <ivbagfpssyirdxuhea@wits.ca>\r\n
Message: MIME-Version: 1.0\r\n

0030 TT 1b 2d 80 00 00 44 61 74 63 3a 20 34 68 75 2c ...Date: Thu,
0040 20 32 32 20 44 65 63 20 32 30 30 35 20 31 35 3a 22 Dec 2005 15:
0050 35 36 3a 35 33 20 2d 30 35 30 30 0d 0a 54 6f 3a 56:53 -0 500..To:
0060 20 22 53 72 75 6c 69 22 20 3c 73 72 75 6c 69 40 "sruli" <sruli@
0070 77 69 74 73 2e 63 61 3e 0d 0a 46 72 6f 6d 3a 20 wits.ca> ..From:
0080 22 53 72 75 6c 69 22 20 3c 73 72 75 6c 69 40 74 "sruli" <sruli@t
0090 69 72 61 6e 61 2e 67 6f 76 2e 61 6c 3e 0d 0a 53 irana.gov.al>..S
00a0 75 62 6a 65 63 74 3a 20 44 61 6e 79 65 6c 6c 0d bject: Danyell.
00b0 0a 4d 65 73 73 61 67 65 2d 49 44 3a 20 3c 69 76 .Message -ID: <iv
00c0 62 61 67 66 70 73 73 79 69 72 64 78 75 68 65 61 bagfpssy irdxuhea
00d0 65 40 77 69 74 73 2e 63 61 3e 0d 0a 4d 49 4d 45 e@wits.c a>..MIME
00e0 2d 56 65 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 43 -version : 1.0..C
00f0 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c ontent-T ype: mul
0100 74 69 70 61 72 74 2f 6d 69 78 65 64 3b 0d 0a 20 tipart/m ixed;..
0110 20 20 20 20 20 20 20 62 6f 75 6e 64 61 72 79 3d b oundary=
0120 22 2d 2d 2d 2d 2d 2d 2d 2d 6d 6a 70 76 6e 6d 6e "----- -mjpgvnmn
0130 68 70 74 76 6c 68 70 69 61 68 7a 77 6b 22 0d 0a hptvlhpi ahzwk"..
0140 0d 0a 2d 6d 6a 70 76 ..----- ----mjpgv
0150 6e 6d 6e 68 70 74 76 6c 68 70 69 61 68 7a 77 6b nmnhotvl hoiahzwk

P: 43914 D: 32 M: 0

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!”

Demonstration Seven

demo

Slow Sign Updates

- Very large, complex system

Microsoft[®]

Sniff and Build Message Sequence Diagram

Microsoft Excel - cmslow.xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

B130 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	

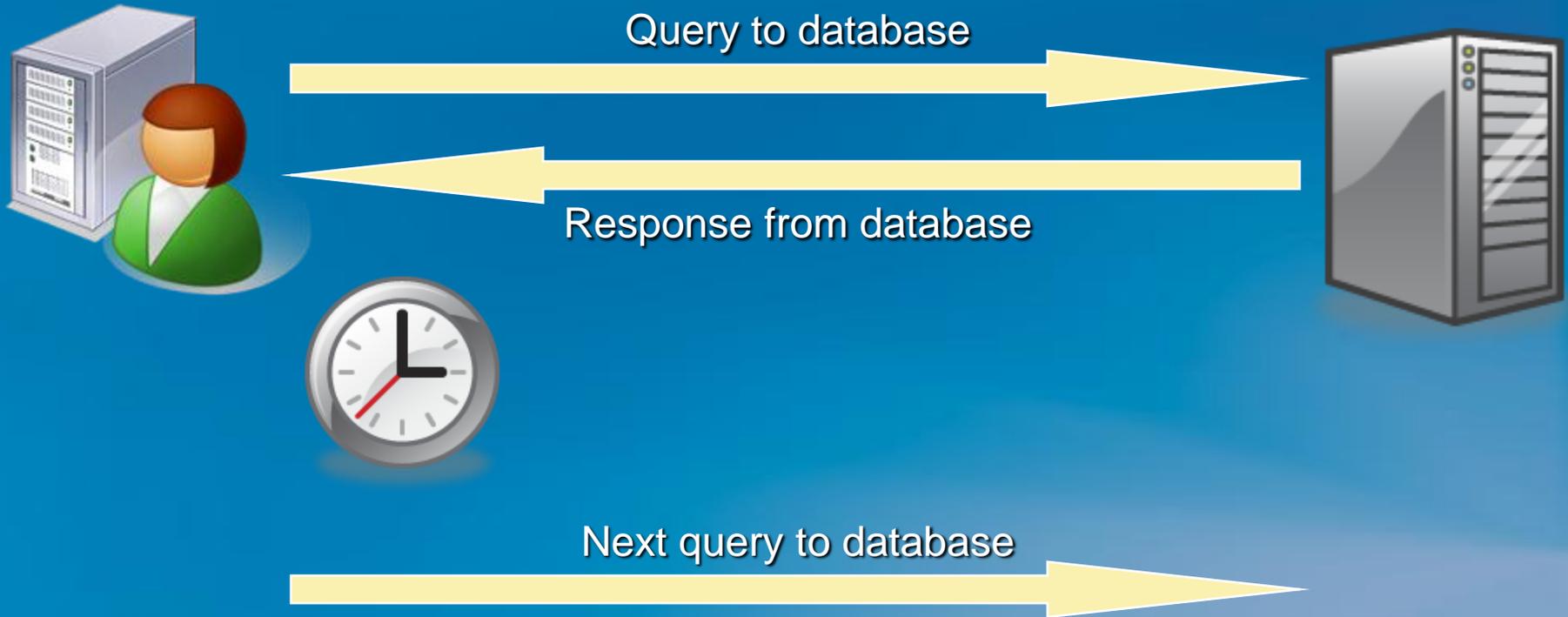
Ready Sum=206.36

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

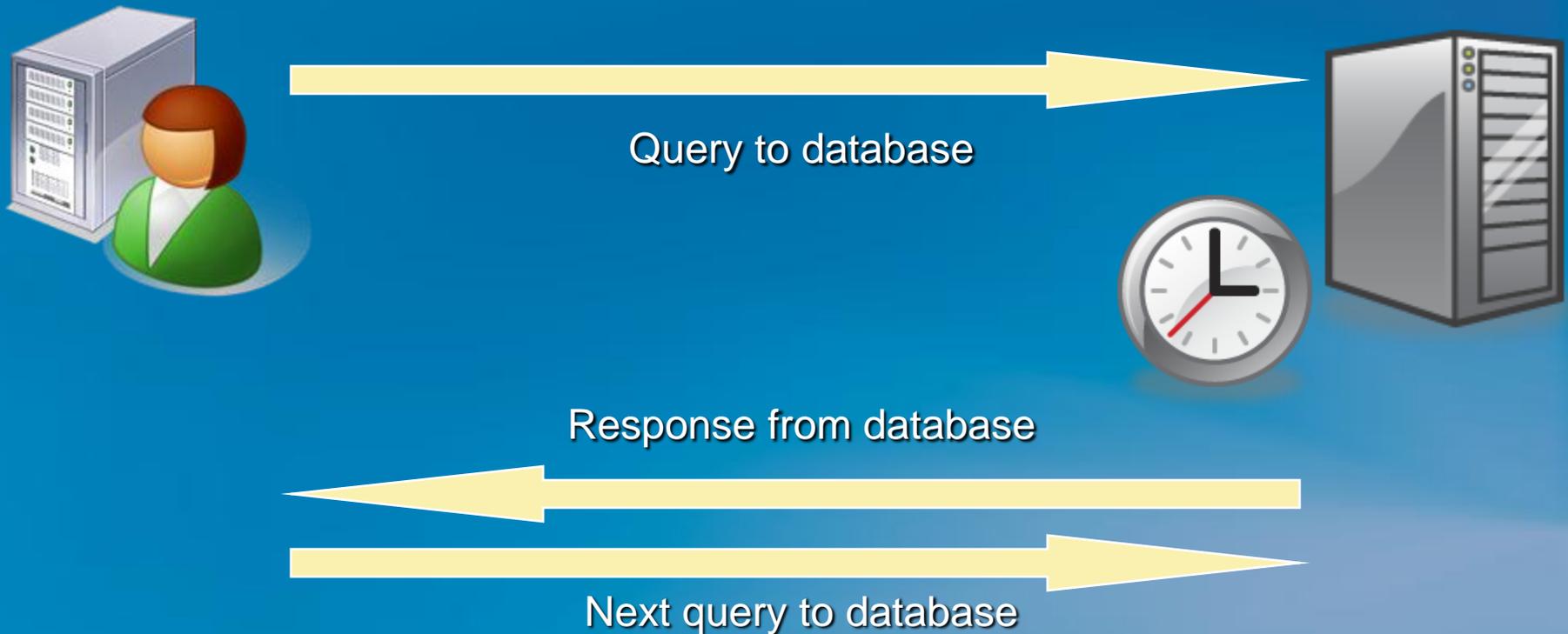
Observations...

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



Observations...

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



Observations...

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

Demonstration Eight

demo

Slow FTP Issue

- First, a good FTP transfer

Microsoft[®]

TCP Data Sequence Diagram

(Transfer already in progress...)

Sender

Packet #53



Receiver

TCP Data Sequence Diagram

(Transfer already in progress...)

Sender

Packet #53

Packet #54



Receiver

TCP Data Sequence Diagram

(Transfer already in progress...)

Sender

Packet #53

Packet #54

Packet #55



Receiver

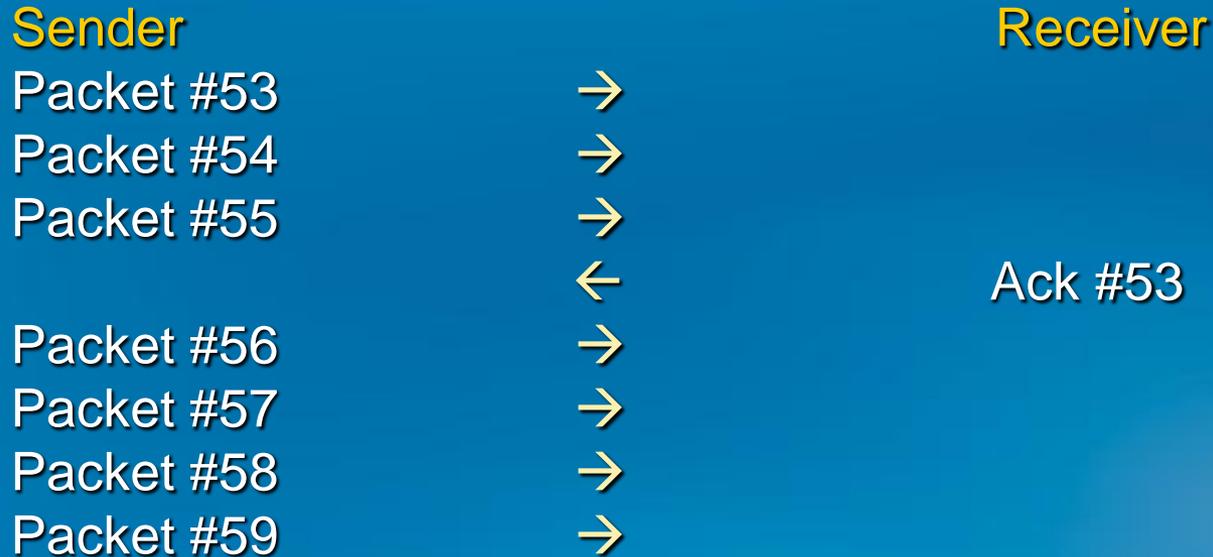
TCP Data Sequence Diagram

(Transfer already in progress...)



TCP Data Sequence Diagram

(Transfer already in progress...)



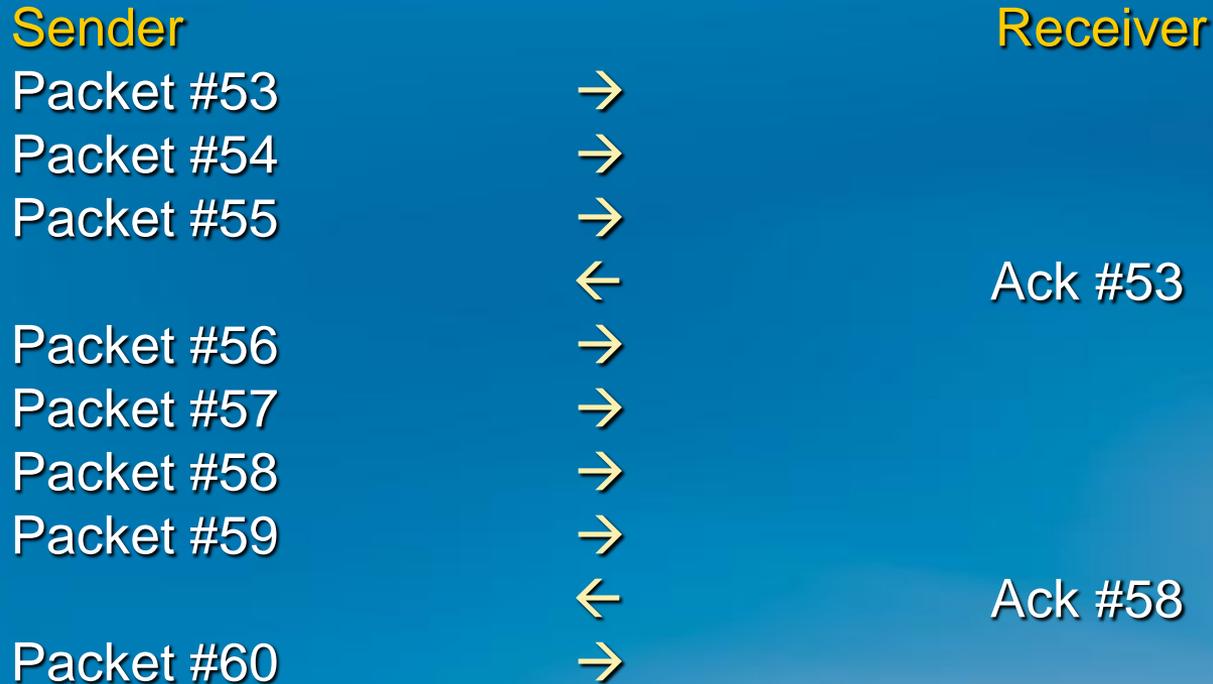
TCP Data Sequence Diagram

(Transfer already in progress...)

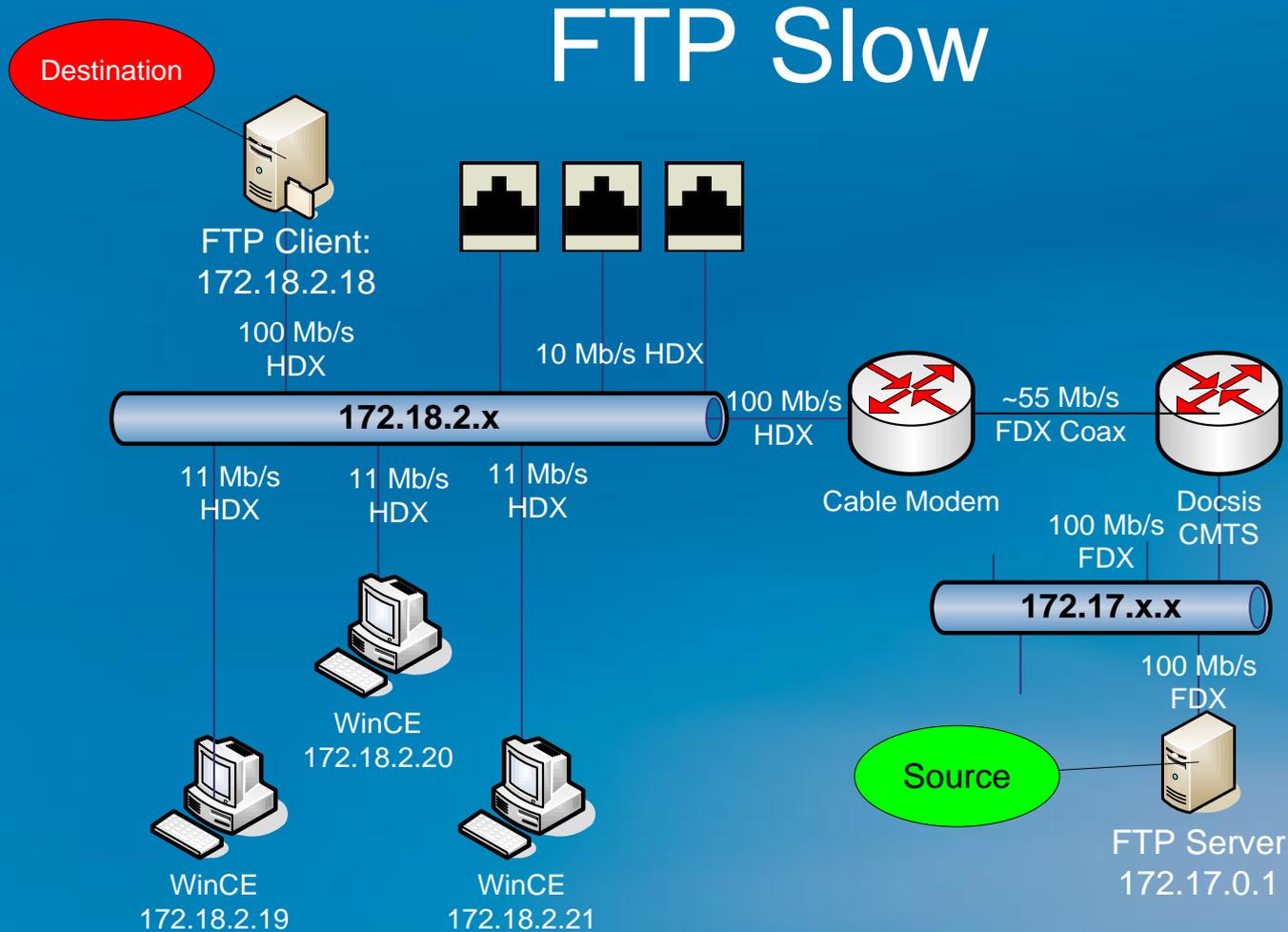


TCP Data Sequence Diagram

(Transfer already in progress...)



Slow FTP Network Diagram



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

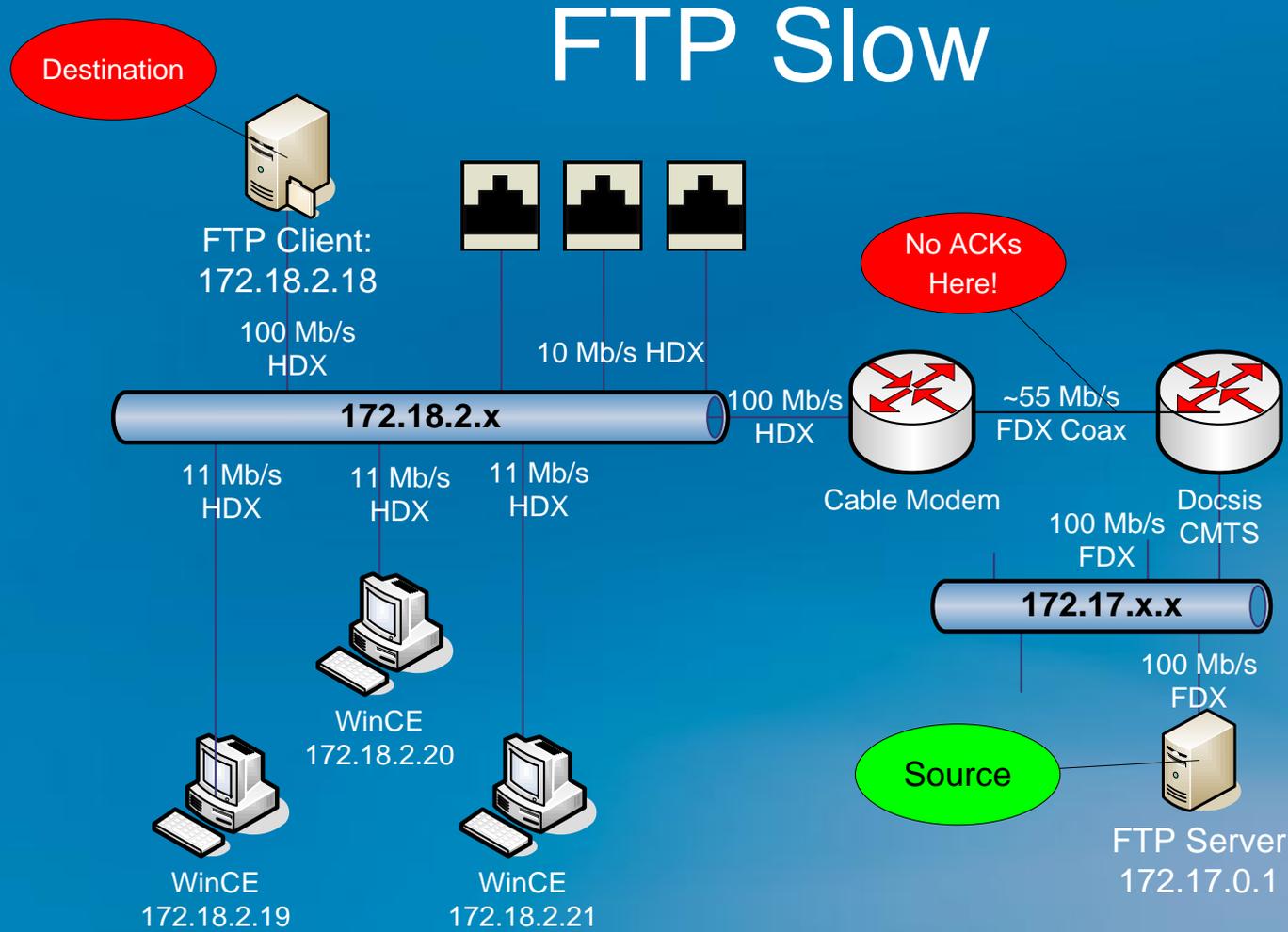
A27

	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



FTP Fails Completely

The screenshot shows the Wireshark interface with a network capture of an FTP session. The packet list pane shows the following details:

No.	Time	Source	Destination	Protocol	Info
33	23.923133	192.168.2.175	newton	FTP-DA	FTP Data: 1398 bytes
34	23.935528	192.168.2.175	newton	FTP-DA	FTP Data: 1398 bytes
35	24.006911	MitsuFWALL	192.168.2.175	ICMP	Destination unreachable (Fragmentation needed)
36	24.034618	MitsuFWALL	192.168.2.175	ICMP	Destination unreachable (Fragmentation needed)
37	24.064491	192.168.2.175	newton	TCP	2500 > ftp [ACK] seq=58 Ack=152 win=16498 Len=0
38	26.868353	192.168.2.175	newton	FTP-DA	[TCP Retransmission] FTP Data: 1398 bytes
39	26.940921	MitsuFWALL	192.168.2.175	ICMP	Destination unreachable (Fragmentation needed)

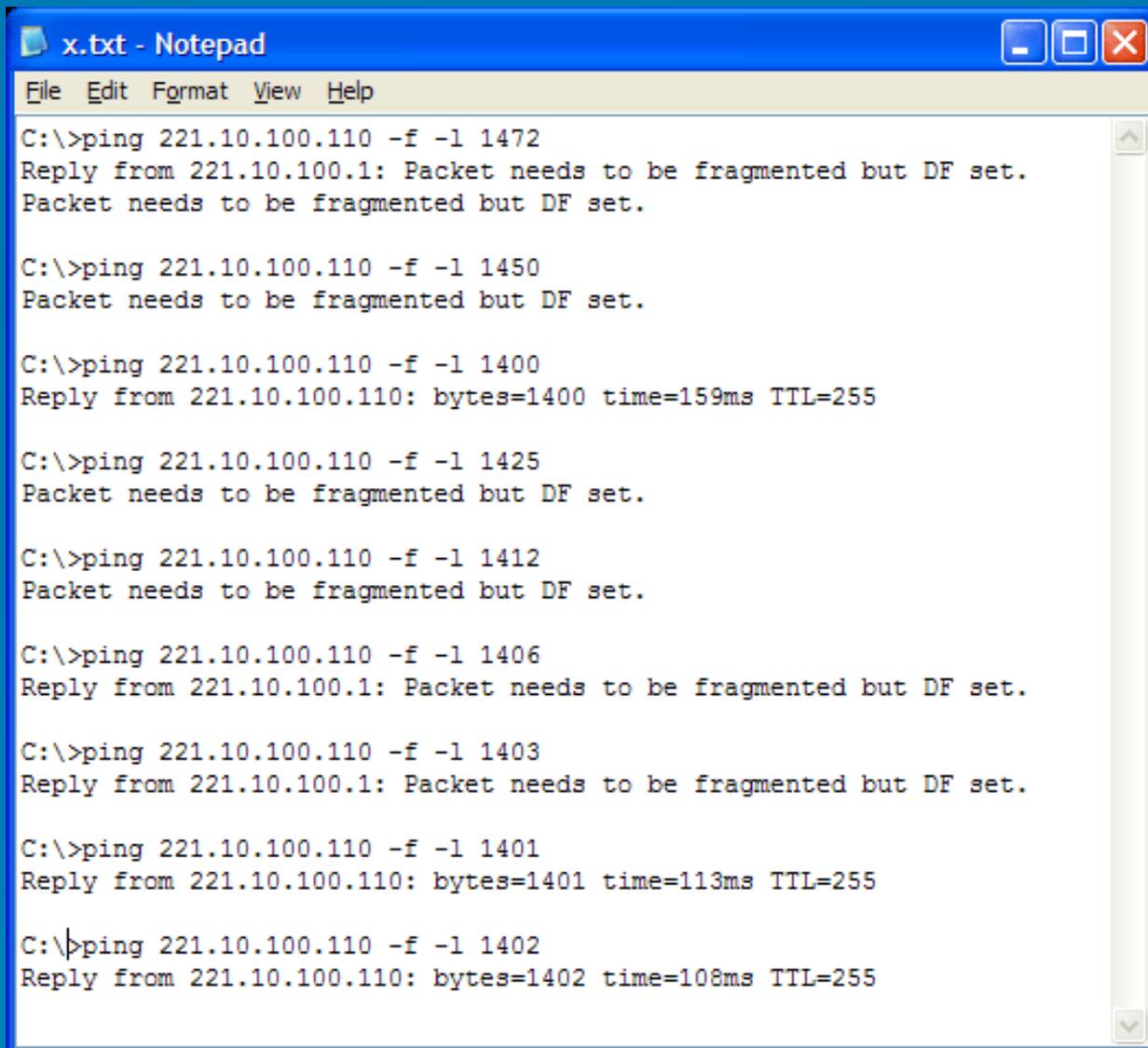
The packet details pane for the selected packet (Frame 7) shows the following layers:

- Frame 7 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: IntelCor_3f:62:d5 (00:15:00:3f:62:d5), Dst: D-Link_55:95:ac (00:0f:3d:55:95:ac)
- Internet Protocol, Src: 192.168.2.175 (192.168.2.175), Dst: newton (221.10.100.110)
- Transmission Control Protocol, Src Port: 2500 (2500), Dst Port: ftp (21), Seq: 0, Ack: 0, Len: 6
- File Transfer Protocol (FTP)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 0f 3d 55 95 ac 00 15 00 3f 62 d5 08 00 45 00  ..=U.... .?b...E.
0010 00 2e 32 f4 40 00 80 06 c3 05 c0 a8 02 af dd 0a  ..2.@... ..
0020 64 6e 09 c4 00 15 d9 7b 3e e7 ce ae 8d e9 50 18  dn.....{ >.....P.
0030 41 0a 2e 79 00 00 58 50 57 44 0d 0a                A..y..XP WD..
```

Fix #1: Find the MTU



```
x.txt - Notepad
File Edit Format View Help
C:\>ping 221.10.100.110 -f -l 1472
Reply from 221.10.100.1: Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1450
Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1400
Reply from 221.10.100.110: bytes=1400 time=159ms TTL=255

C:\>ping 221.10.100.110 -f -l 1425
Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1412
Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1406
Reply from 221.10.100.1: Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1403
Reply from 221.10.100.1: Packet needs to be fragmented but DF set.

C:\>ping 221.10.100.110 -f -l 1401
Reply from 221.10.100.110: bytes=1401 time=113ms TTL=255

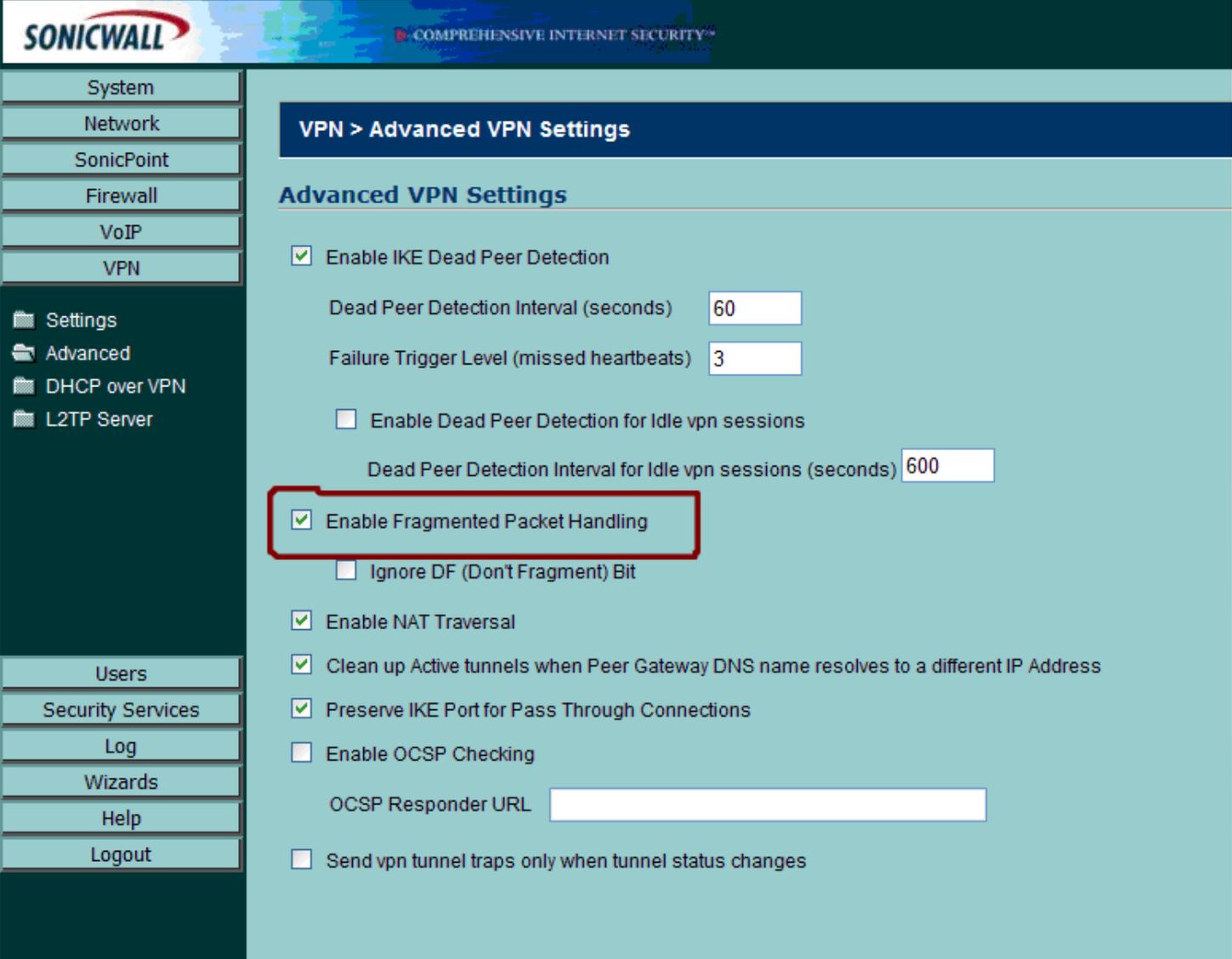
C:\>ping 221.10.100.110 -f -l 1402
Reply from 221.10.100.110: bytes=1402 time=108ms TTL=255
```

...Then Set Your Net Interface

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure, with the path expanded to: `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C6373FF0-2456-45A3-9B2E-E8E519356}`. The right pane shows a list of registry values for this interface.

Name	Type	Data
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
IPAddress	REG_MULTI_SZ	0.0.0.0
IPAutoconfigurationAddress	REG_SZ	0.0.0.0
IPAutoconfigurationMask	REG_SZ	255.255.0.0
IPAutoconfigurationSeed	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x0002a300 (172800)
LeaseObtainedTime	REG_DWORD	0x45b20a28 (1169295912)
LeaseTerminatesTime	REG_DWORD	0x45b4ad28 (1169468712)
NameServer	REG_SZ	
NTEContextList	REG_MULTI_SZ	0x00000003
RawIPAllowedProtocols	REG_MULTI_SZ	0
RegisterAdapterName	REG_DWORD	0x00000000 (0)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
SubnetMask	REG_MULTI_SZ	0.0.0.0
T1	REG_DWORD	0x45b35ba8 (1169382312)
T2	REG_DWORD	0x45b458c8 (1169447112)
TCPAllowedPorts	REG_MULTI_SZ	0
UDPAllowedPorts	REG_MULTI_SZ	0
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
MTU	REG_DWORD	0x000004e2 (1250)

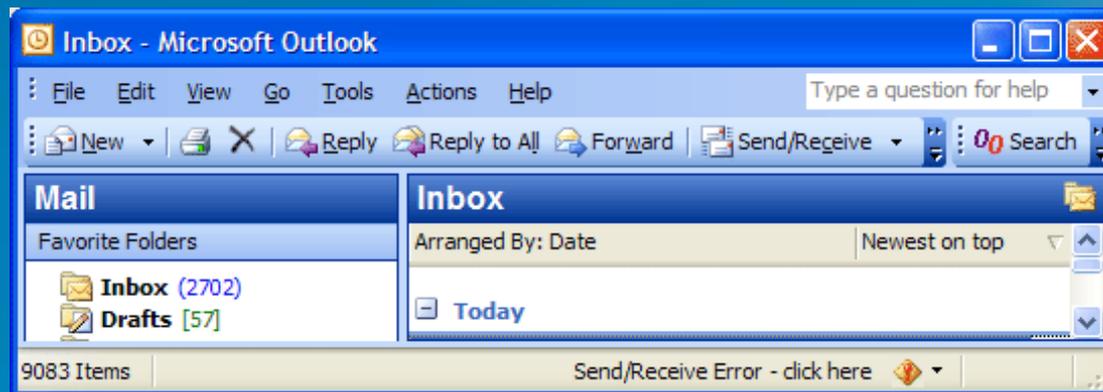
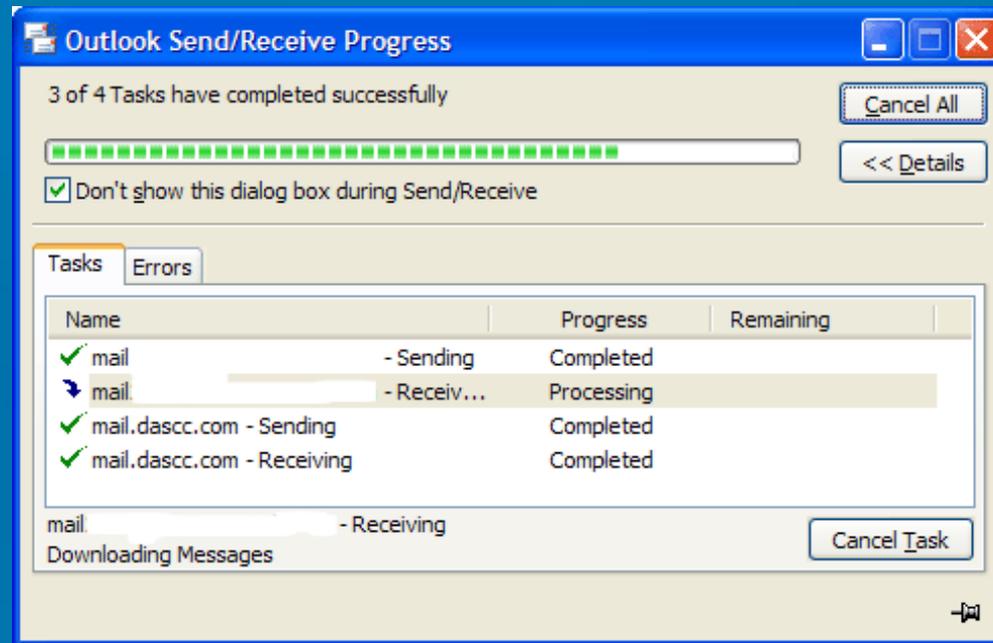
Fix #2: Allow Fragmentation



The screenshot shows the SonicWall management interface. The left sidebar contains a navigation menu with the following items: System, Network, SonicPoint, Firewall, VoIP, VPN, Settings, Advanced, DHCP over VPN, L2TP Server, Users, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'VPN > Advanced VPN Settings' and 'Advanced VPN Settings'. The settings are as follows:

- Enable IKE Dead Peer Detection
 - Dead Peer Detection Interval (seconds)
 - Failure Trigger Level (missed heartbeats)
 - Enable Dead Peer Detection for Idle vpn sessions
 - Dead Peer Detection Interval for Idle vpn sessions (seconds)
- Enable Fragmented Packet Handling
 - Ignore DF (Don't Fragment) Bit
- Enable NAT Traversal
- Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address
- Preserve IKE Port for Pass Through Connections
- Enable OCSP Checking
 - OCSP Responder URL
- Send vpn tunnel traps only when tunnel status changes

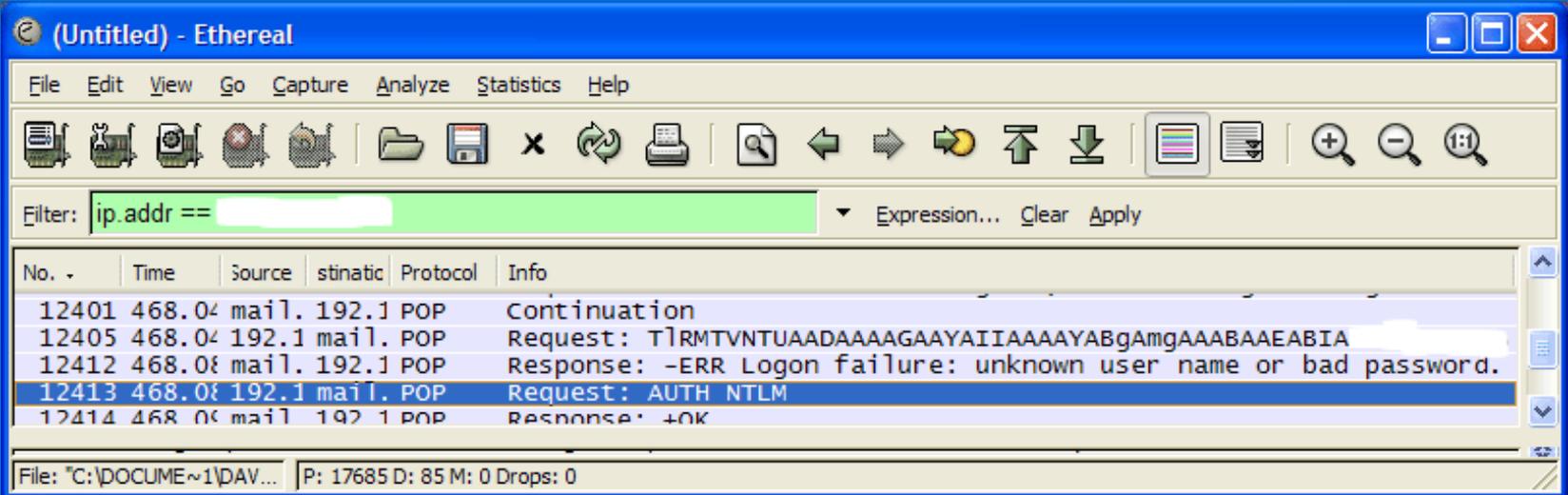
“My Mail Is Timing Out...”



“My Mail Is Timing Out... Why?”



“My Mail Is Timing Out... Why?”



The screenshot shows the Wireshark interface with a filter applied to capture traffic from a specific IP address. The packet list pane displays several POP3 protocol messages. The most significant message is a response from the mail server indicating a login failure due to an unknown user name or bad password.

No.	Time	Source	Destination	Protocol	Info
12401	468.04	mail.192.1	192.1	POP	Continuation
12405	468.04	192.1	mail.192.1	POP	Request: T1RMTVNTUAAADAAAAGAAAYAIIAAAAYABgAmgAAABAAEABIA
12412	468.08	mail.192.1	192.1	POP	Response: -ERR Logon failure: unknown user name or bad password.
12413	468.08	192.1	mail.192.1	POP	Request: AUTH NTLM
12414	468.08	mail.192.1	192.1	POP	Response: +OK

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!

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

For More Information

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

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[®]