



Troubleshooting: The Network is Slow

Laura Chappell
Protocol Analysis Institute, Inc.

lchappell@packet-level.com

www.packet-level.com

www.podbooks.com

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Course Contents

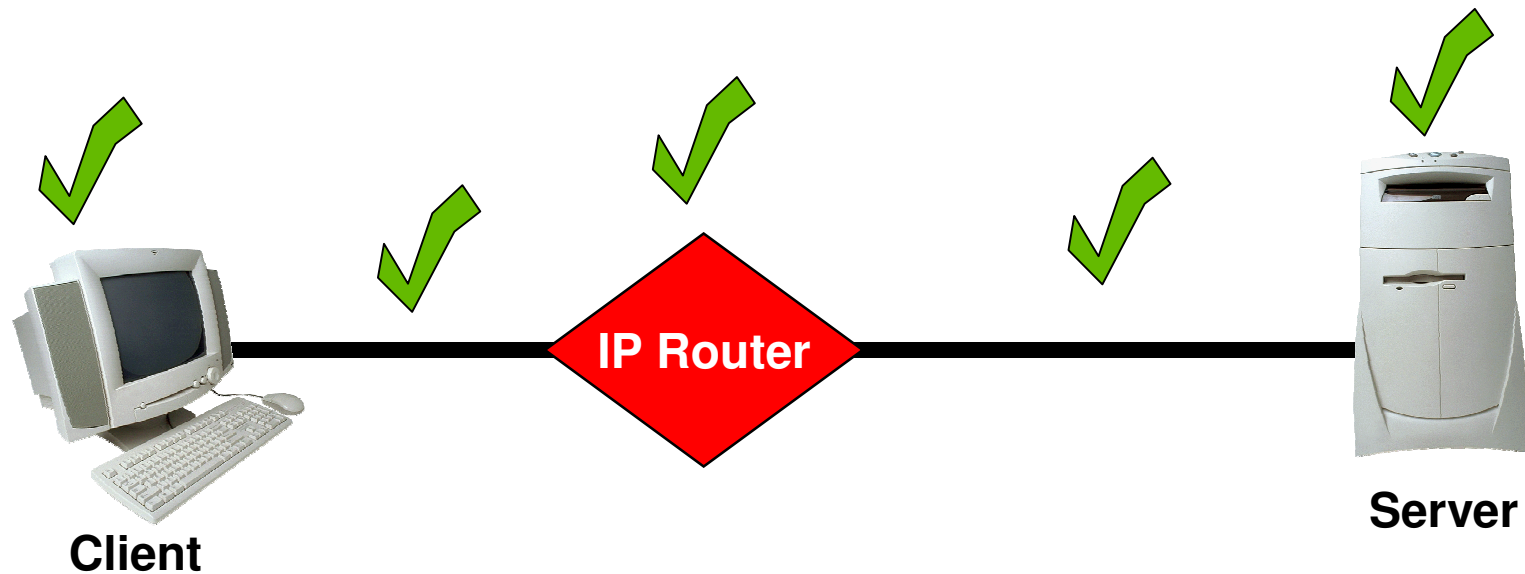
- The onsite process
- Typical network map
- Client information
- Defining “slow”
- Testing your latency
- The “laying on of hands”
- Client analysis
- Application Analysis Form (AAF)
- Analyzing the login sequence
- Looking for consistency
- Working backwards to ID the problem

The Onsite Process to Troubleshoot *“The Network is Slow”* Problem



- Prerequisites
 - Review the Network map
 - Identify the tap-in point information
 - Ask about the slowness characteristics
- Process
 - The “Laying On Of Hands”
 - Latency tests
 - The client bootup/login analysis process
 - The application analysis process

The “Network” is Slow?



Client fault (process problems, no connection, etc.)

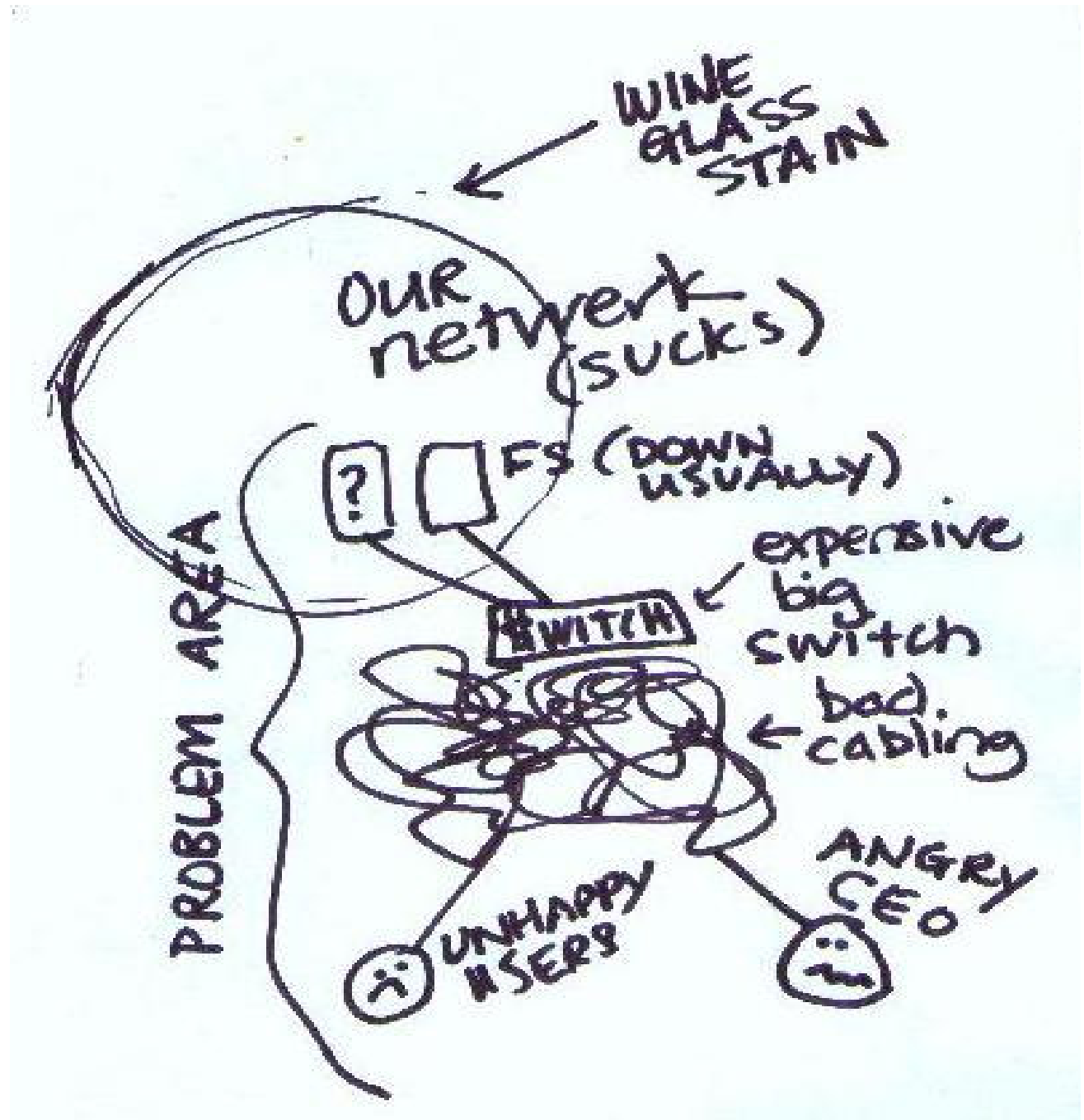
Local link fault (high latency, retransmissions, no route, etc.)

Route fault (high latency, no route, discard, etc.)

Remote link fault (high latency, retransmissions, no route, etc.)

Server fault (process problems, no connection, error response, etc.)

Typical Network Map



Client Information

- Define “slow”?
- Slow for whom?
- Application-specific?
- Network segment-specific?
- Intermittent? Constant?
- Can you replicate the problem?

Client #1 Information

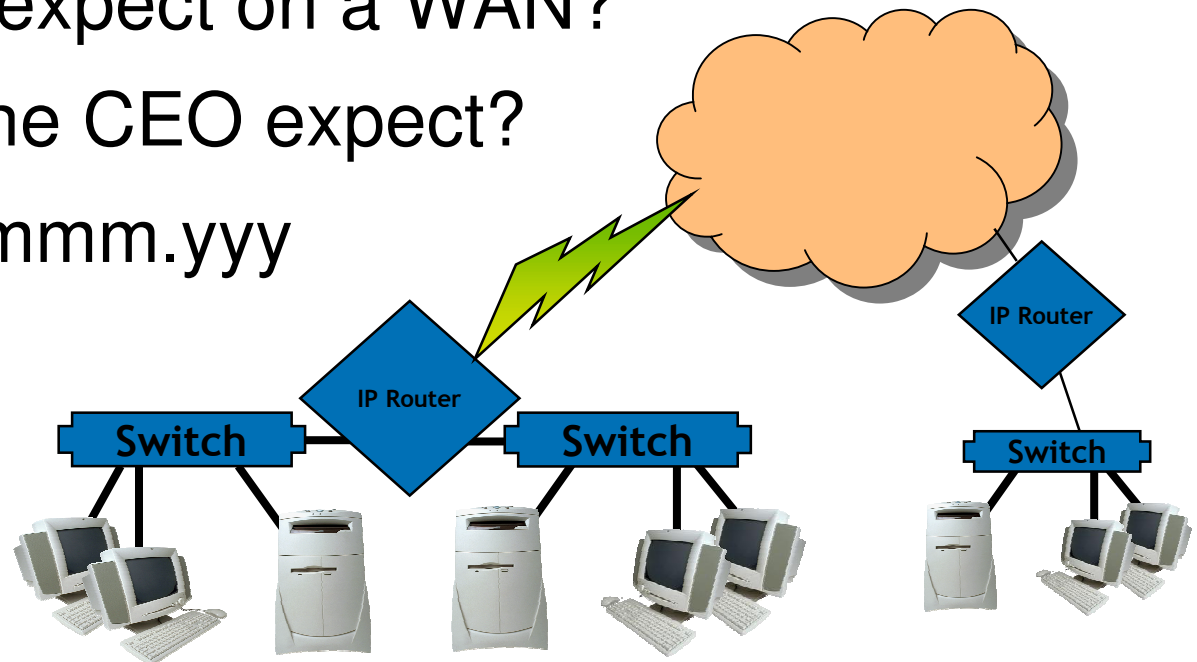
- Define “slow”?
 - Slow for whom?
 - Application-specific?
 - Network segment-specific?
 - Intermittent? Constant?
 - Can you replicate the problem?
- Lousy... stinky...
Everyone
All
Nope
Constant
Yes

“Slow” Is Relative

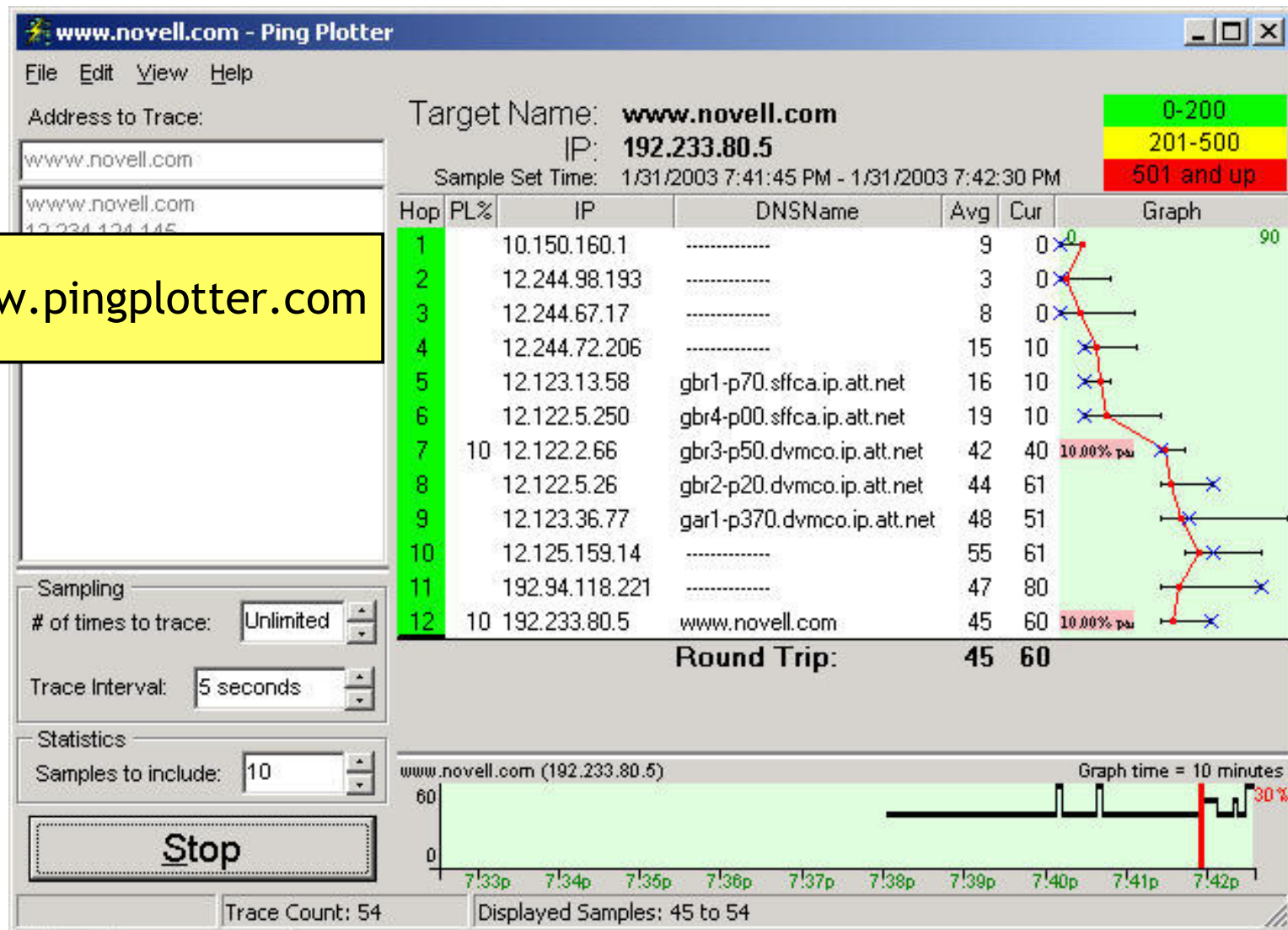
- What do we expect on a LAN?
- What do we expect on a WAN?
- What does the CEO expect?
- HH:MM:SS.mmm.yyy

– Where

- HH = hours
- MM = minutes
- SS = seconds
- mmm = milliseconds (thousandths of a second)
- yyy = microseconds (millionths of a second)

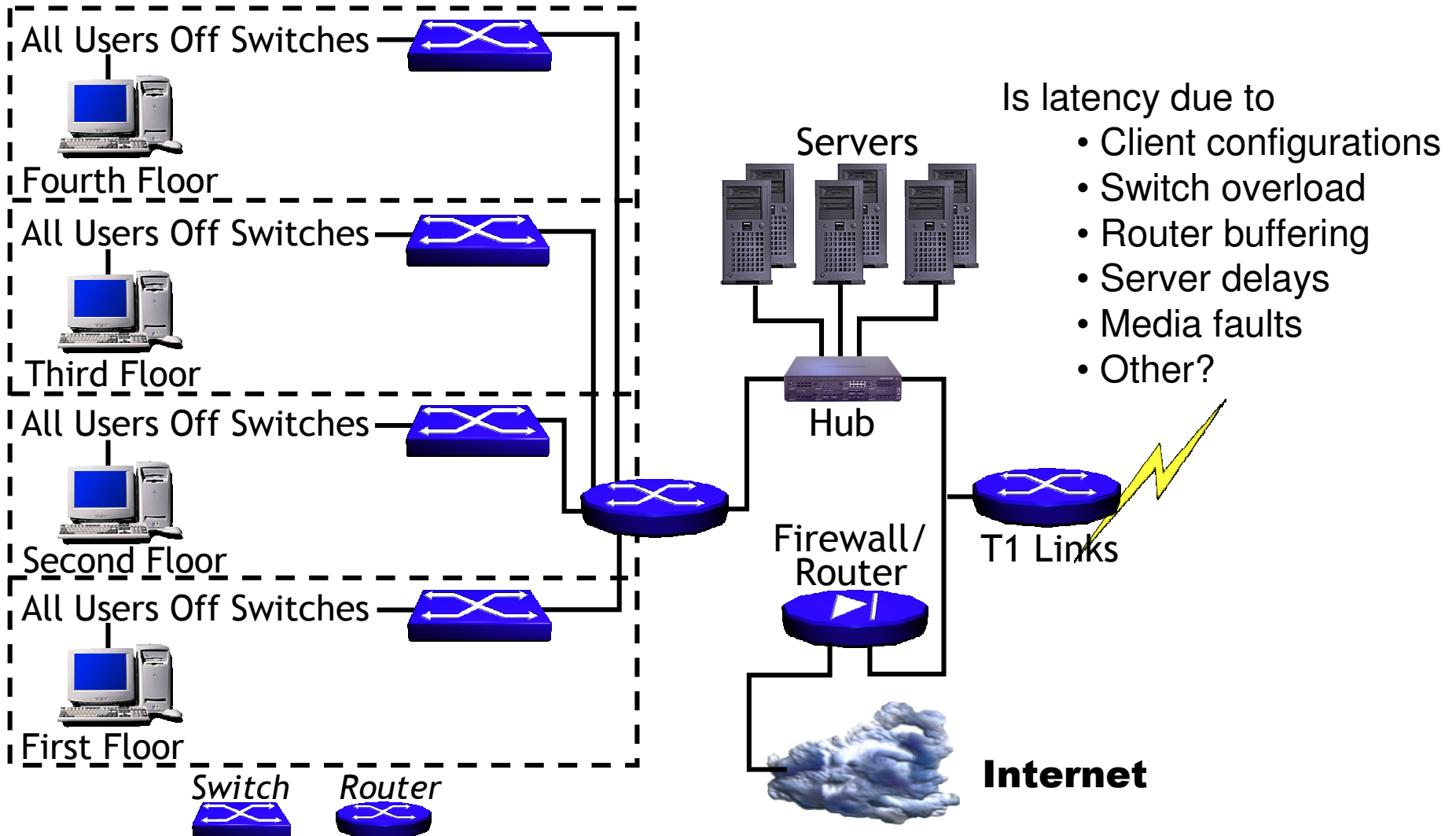


Test Your Own Latency



www.pingplotter.com

OK – A Better Network Diagram

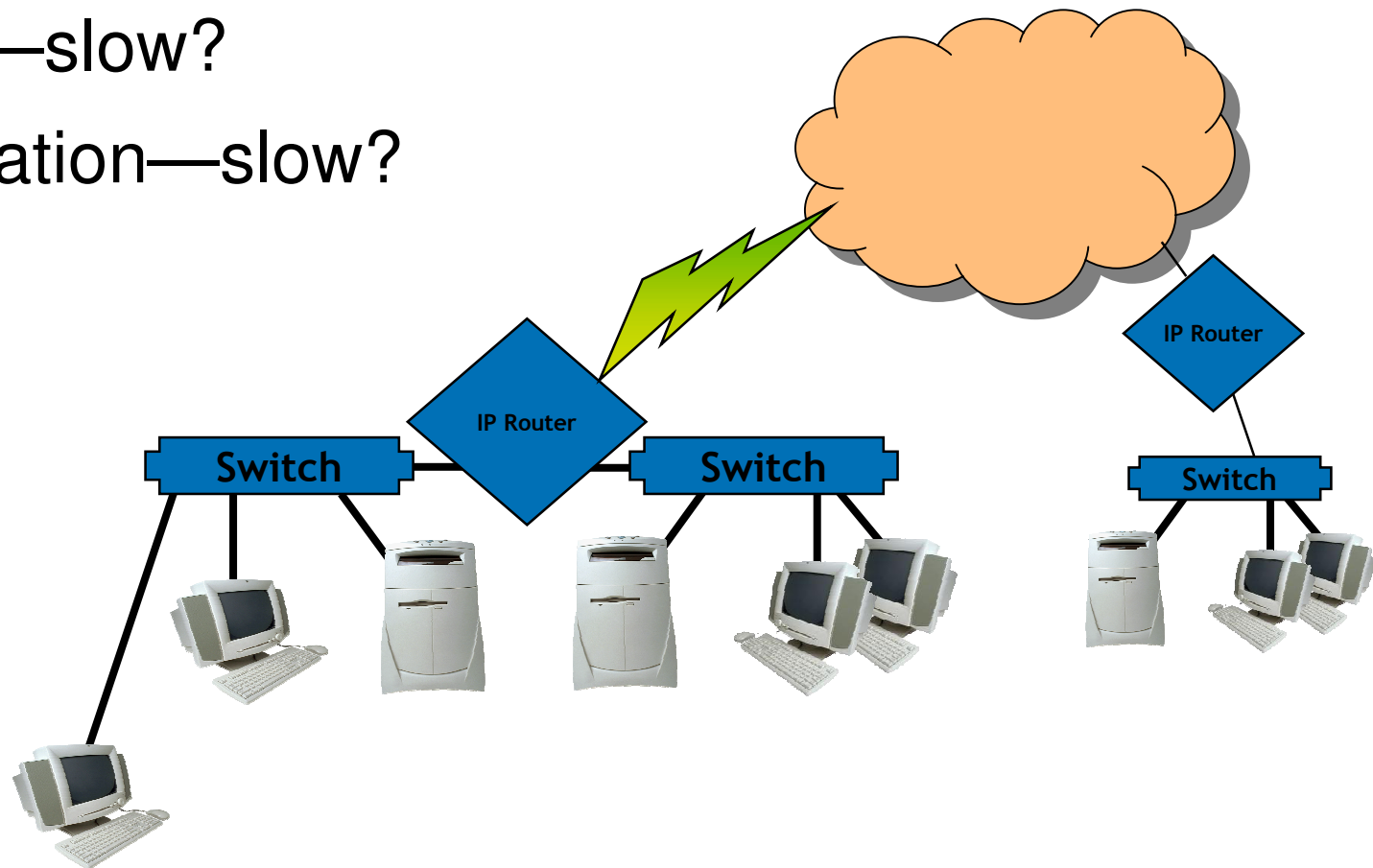


Laying On Of Hands

- Broadcast/multicast storms?
- Excessive ICMP traffic?
- Rogue traffic?
- General network conditions?
- Server delay packets (spanning required)?
- Retransmissions-media faults (spanning required)?

Performing The Client Analysis

- Bootup—slow?
- Login—slow?
- Application—slow?



The Application Analysis Form

- Simple format

**DON'T TOUCH
THE
KEYBOARD!**

elsie

Elsie's Startup/Email

| Start Pkt | General | Stop Pkt |
|-------------|---|-------------|
| <i>0</i> | Process: <i>BOOT UP</i> <i>NO HANDS</i> Time: <i>.57</i> Packets: <i>383</i> | <i>383</i> |
| <i>384</i> | Process: <i>LOGIN</i> Time: <i>.24</i> Packets: <i>1545</i> | <i>1929</i> |
| <i>1930</i> | Process: <i>LAUNCH NSN</i> Time: <i>.376</i> Packets: <i>5</i> | <i>1935</i> |
| <i>1936</i> | Process: <i>EMAIL OPEN</i> Time: <i>1.14</i> Packets: <i>268</i> | <i>2204</i> |
| <i>2205</i> | Process: <i>READ 1</i> Time: <i>.04</i> Packets: <i>201</i> | <i>2406</i> |
| <i>2407</i> | Process: <i>CLOSE MAIL PGM</i> Time: <i>1.12</i> Packets: <i>526</i> | <i>2933</i> |
| | Process: _____ Time: _____ Packets: _____ | |
| | Process: _____ Time: _____ Packets: _____ | |
| | Process: _____ Time: _____ Packets: _____ | |
| | Process: _____ Time: _____ Packets: _____ | |
| | Process: _____ Time: _____ Packets: _____ | |
| | Process: _____ Time: _____ Packets: _____ | |

Handwritten notes:

- DHCP problem -> dups*
- good firewall*
- Navigator home page = null*
- slow response pop*
- really slow close: appears hung*
- close out*

Application Analysis Form

Start pkt

End pkt

| |
|---|
| 0 |
|---|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| |
|--|
| |
|--|

Application Analysis Form

Start pkt

End pkt

0

Bootup

385

386

Application Analysis Form

Start pkt

End pkt

0

Bootup

385

386

Login

1929

Elsie's Login Sequence

- Look for time irregularities.

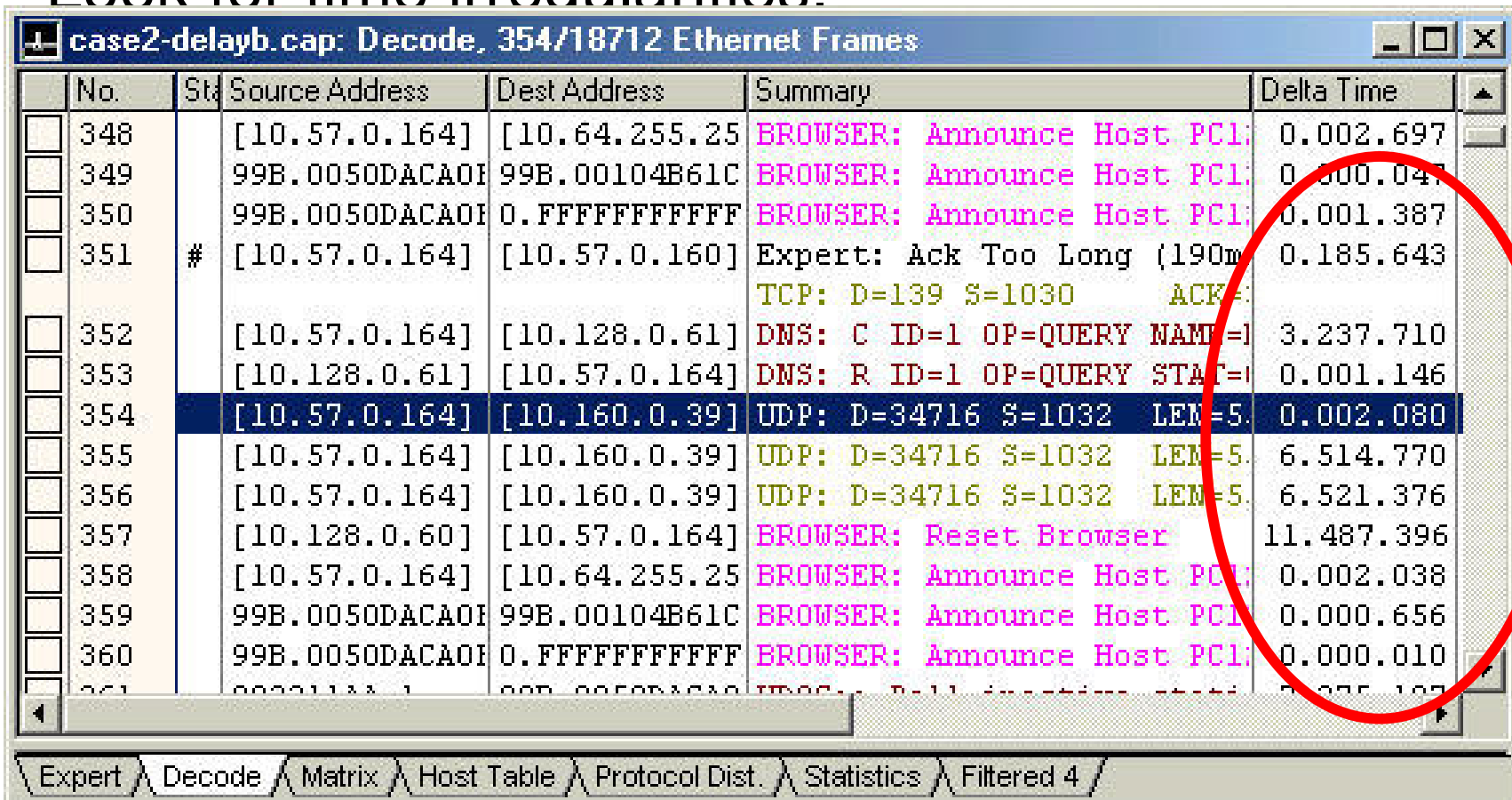
| case2-delayb.cap: Decode, 354/18712 Ethernet Frames | | | | | | |
|---|-----|----------------|----------------|---|------------|--|
| No. | Sta | Source Address | Dest Address | Summary | Delta Time | |
| 348 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.697 | |
| 349 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.047 | |
| 350 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.001.387 | |
| 351 | # | [10.57.0.164] | [10.57.0.160] | Expert: Ack Too Long (190m: TCP: D=139 S=1030 ACK= | 0.185.643 | |
| 352 | | [10.57.0.164] | [10.128.0.61] | DNS: C ID=1 OP=QUERY NAME= | 3.237.710 | |
| 353 | | [10.128.0.61] | [10.57.0.164] | DNS: R ID=1 OP=QUERY STAT= | 0.001.146 | |
| 354 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 0.002.080 | |
| 355 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.514.770 | |
| 356 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.521.376 | |
| 357 | | [10.128.0.60] | [10.57.0.164] | BROWSER: Reset Browser | 11.487.396 | |
| 358 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.038 | |
| 359 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.656 | |
| 360 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.000.010 | |

Delta/interpacket: Time from end of one packet to end of next packet.

Relative: Relative to first or marked packet.

Elsie's Login Sequence

- Look for time irregularities.



| No. | Sta | Source Address | Dest Address | Summary | Delta Time |
|-----|-----|----------------|----------------|--|------------|
| 348 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.697 |
| 349 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.047 |
| 350 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.001.387 |
| 351 | # | [10.57.0.164] | [10.57.0.160] | Expert: Ack Too Long (190m TCP: D=139 S=1030 ACK= | 0.185.643 |
| 352 | | [10.57.0.164] | [10.128.0.61] | DNS: C ID=1 OP=QUERY NAME= | 3.237.710 |
| 353 | | [10.128.0.61] | [10.57.0.164] | DNS: R ID=1 OP=QUERY STAT= | 0.001.146 |
| 354 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 0.002.080 |
| 355 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.514.770 |
| 356 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.521.376 |
| 357 | | [10.128.0.60] | [10.57.0.164] | BROWSER: Reset Browser | 11.487.396 |
| 358 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.038 |
| 359 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.656 |
| 360 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.000.010 |

Expert Decode Matrix Host Table Protocol Dist. Statistics Filtered 4

Delta/interpacket: Time from end of one packet to end of next packet.

Relative: Relative to first or marked packet.

Look for Consistencies

- First... look for other time problems
- Then... look for the surrounding packets

| case2-delayb.cap: Decode, 3210/18712 Ethernet Frames | | | | | | |
|--|------|-----|----------------|----------------|-----------------------------|------------|
| | No. | Sta | Source Address | Dest Address | Summary | Delta Time |
| <input type="checkbox"/> | 3206 | | 99B.0050DACA0F | 971119A3.1 | NCP: C Get file/subdir info | 0.001.024 |
| <input type="checkbox"/> | 3207 | | 971119A3.1 | 99B.0050DACA0F | NCP: R OK, Got info | 0.000.767 |
| <input type="checkbox"/> | 3208 | # | 99B.0050DACA0F | 971119A3.1 | Expert: Loops on same requ | 0.000.733 |
| <input type="checkbox"/> | 3209 | | 971119A3.1 | 99B.0050DACA0F | NCP: R OK, Got info | 0.001.080 |
| <input type="checkbox"/> | 3210 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 0.004.588 |
| <input type="checkbox"/> | 3211 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 6.511.047 |
| <input type="checkbox"/> | 3212 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 6.519.300 |
| <input type="checkbox"/> | 3213 | | 99B.0050DACA0F | 971119A3.1 | NBURST: C F=CBA20900 Burst | 6.523.176 |
| <input type="checkbox"/> | 3214 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R OK 1412 bytes re | 0.002.941 |
| <input type="checkbox"/> | 3215 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.149 |
| <input type="checkbox"/> | 3216 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.002.300 |
| <input type="checkbox"/> | 3217 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.147 |
| <input type="checkbox"/> | 3218 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.002.294 |
| <input type="checkbox"/> | 3219 | | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.154 |

Look for Consistencies

- First... look for other time problems
- Then... look for the surrounding packets

18 second
delay every
90 seconds
(approx.)
- all users -

| | Source Address | Dest Address | Summary | Delta Time |
|-------------------------------|----------------|----------------|------------------------------|------------|
| | 9B.0050DACA0F | 971119A3.1 | NCP: C Get file/subdir info | 0.001.024 |
| | 711119A3.1 | 99B.0050DACA0F | NCP: R OK, Got info | 0.000.767 |
| | 9B.0050DACA0F | 971119A3.1 | Expert: Loops on same req | 0.000.733 |
| | 711119A3.1 | 99B.0050DACA0F | NCP: C Get file/subdir info | 0.001.080 |
| | 711119A3.1 | 99B.0050DACA0F | NCP: R OK, Got info | 0.001.080 |
| <input type="checkbox"/> 3210 | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 0.004.588 |
| <input type="checkbox"/> 3211 | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 6.511.047 |
| <input type="checkbox"/> 3212 | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1036 LEN=5 | 6.519.300 |
| <input type="checkbox"/> 3213 | 99B.0050DACA0F | 971119A3.1 | NBURST: C F=CBA20900 Burst | 6.523.176 |
| <input type="checkbox"/> 3214 | 971119A3.1 | 99B.0050DACA0F | NBURST: R OK 1412 bytes read | 0.002.941 |
| <input type="checkbox"/> 3215 | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.149 |
| <input type="checkbox"/> 3216 | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.002.300 |
| <input type="checkbox"/> 3217 | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.147 |
| <input type="checkbox"/> 3218 | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.002.294 |
| <input type="checkbox"/> 3219 | 971119A3.1 | 99B.0050DACA0F | NBURST: R 1420 bytes read | 0.000.158 |

Work Backwards To ID Process

- Ping 10.160.0.39 – no answer
- What made the client send a packet to that address?

| No. | Sta | Source Address | Dest Address | Summary | Delta Time |
|-----|-----|----------------|----------------|----------------------------|------------|
| 348 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.697 |
| 349 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.047 |
| 350 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.001.387 |
| 351 | # | [10.57.0.164] | [10.57.0.160] | Expert: Ack Too Long (190m | 0.185.643 |
| 352 | | [10.57.0.164] | [10.128.0.61] | TCP: D=139 S=1030 ACK=. | 3.237.710 |
| 353 | | [10.128.0.61] | [10.57.0.164] | DNS: R ID=1 OP=QUERY STAT= | 0.001.146 |
| 354 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 0.002.080 |
| 355 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.514.770 |
| 356 | | [10.57.0.164] | [10.160.0.39] | UDP: D=34716 S=1032 LEN=5 | 6.521.376 |
| 357 | | [10.128.0.60] | [10.57.0.164] | BROWSER: Reset Browser | 11.487.396 |
| 358 | | [10.57.0.164] | [10.64.255.25] | BROWSER: Announce Host PC1 | 0.002.038 |
| 359 | | 99B.0050DACA0F | 99B.00104B61C | BROWSER: Announce Host PC1 | 0.000.656 |
| 360 | | 99B.0050DACA0F | 0.FFFFFFFF | BROWSER: Announce Host PC1 | 0.000.010 |

Work Backwards To ID Process

- In this case, a UDP transmission was triggered by a local application looking for a remote service that did not exist at the destination IP address.



SAP for service →
DNS name resolution →
← DNS server answers
Client babbles away →



Additional Trace Files

- Look for
 - Failures
 - Duplications
 - High latencies
 - Unrecognized traffic
 - Other strange behavior

Keep Those Traces!

- Calculate the ROI
- Great evidence!
- Fun reading!
- Good jokes at bars!



Ref

Get the Analysis ROI Worksheet!

Conclusion

- Get the primary directive
- Get a decent network map
- Perform the “laying on of hands” first
- Consider hubbing out to the client
- Use the Application Analysis Form to help organize your trace files
- Keep your traces!