SHARKFEST '13

Wireshark Developer and User Conference

Using Wireshark as an Application Support Engineer

Tim Poth
Senior Priority Response Analyst
Bentley Systems, Inc.
tim.poth@bentley.com

Agenda

- Quick intro to Bentley Systems, Inc
- How the Priority Response Team (PRT), uses Wireshark to support our applications and users
- Quick intro to the Bentley Products in use when the captures were made
- Look at Wireshark captures

About Bentley Systems

- Bentley is the global leader dedicated to providing architects, engineers, constructors, and owner-operators with comprehensive software solutions for sustaining infrastructure
- Core Products my group deals with
  - MicroStation, CAD platform: if you have seen AutoCAD, it's the same thing only better
  - ProjectWise: Document management system that understands / tracks references in engineering documents
  - AssetWise: Manage asset lifecycles with assured information integrity

Introduction to PRT

- PRT is the buffer between Support and Product Development
- We deal with problems ranging from configuration issues to crash dump analysis
- We primarily supports 2 applications with Wireshark; ProjectWise and SelectServer
  - ProjectWise – we already introduced this
  - SelectServer – licensing server, records product usage

Why do we use Wireshark

- When a company has a problem with our applications we often have to work with the end user or application admin, not a network admin
- We use Wireshark to understand how our application is behaving on their network and to track down obstacles preventing it from working correctly
- Sometimes we find broken devices, configuration issues, software bugs
- Wireshark helps us ‘prove’ where / what the problem is and get it fixed

How do we capture with Wireshark

- For easy / quick to reproduce issues we will often just fire up the Wireshark GUI
- For anything that takes a lot of time or generates a lot of traffic will run Dumpcap
  - For longer running capture we will normally use a circular buffer as large as we can get away with
  - If space is an issue we will filter what we capture but we rarely do
- Tshark is almost never used but if we are looking for something very specific it can be helpful

Where do we capture

- We normally start on the clients PC and move to the server(s) the client is connecting to if needed
- If just client and server do not provide enough info we push users IT to capture anywhere and everywhere they can (routers, firewalls, Riverbed Steelheads, span ports to laptops)

About ProjectWise

- ProjectWise is a Client / Server application
- Uses a proprietary protocol on TCP Port 5800 (nothing to do with VNC)
- Each file transfer session starts a new TCP Connection using TCP port 5800 (newer version does reuse connections for a batch of files)
- Supports application specific “gateways” and “routing” - Server roles – Integration, Gateway, Caching, Web

About ProjectWise – Part 2

- A Datasource is a collection of folders / metadata hosted on a server, one server can have many Datasources, each Datasource can have many file storage locations

About SelectServer

- IIS / .NET application that processes / records product usages in a database
- Usage data is communicated via SOAP over HTTP(S)
- Some of the POST requests return a 500 as normal behavior
- Bentley hosts a public instance on the internet, clients can also deploy a locally instance. Local servers send usage data to public instance

About eB Insight

- Component of Bentleys AssetWise product
- IIS / Web browser based document / asset management system with emphasis on life cycle and change management
- ActiveX file transfer component

Quick Plugs

- CloudShark.org
  - Wireshark in a browser, useful for sharing captures with a group
  - They sent me a hat
- Gliffy.com
  - Web based diagram / flowchart software
  - Can be used for free, I have used them to create the diagrams in my presentations for the last 3 years

Last Notes

- This is a participation required session, speak up, ask questions
- Consider 1.*.*.* as a valid internet IP address

It is the network

1 – PW file upload fails

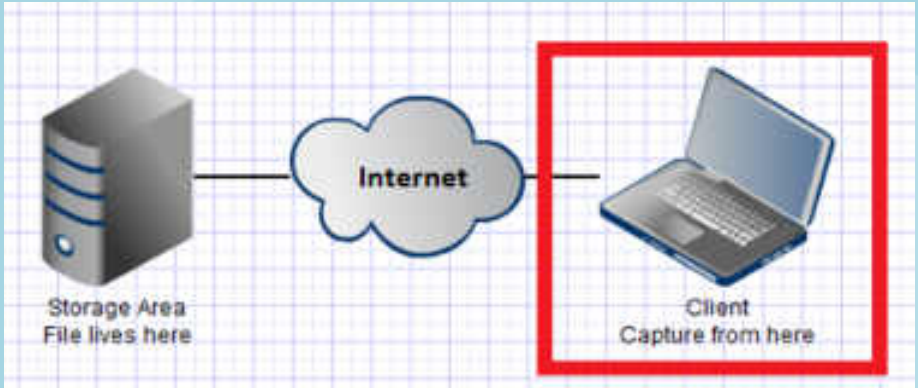
- Several user at different sites having issues connecting / uploading files to a internet facing ProjectWise Server
- Client and Server logs both show unexpected reset
- Log Snip

2012-07-16 09:07:04,012 pwise.ft.stream - sending block 3863, size = 32772 …

2012-07-16 09:07:04,012 pwise.socket - socket_send: starting send() bytes: 32772 flags: 0

2012-07-16 09:07:23,125 pwise.socket - Error -10054 on socket 2204 …

-10054 is "WSAE CONN RESET"

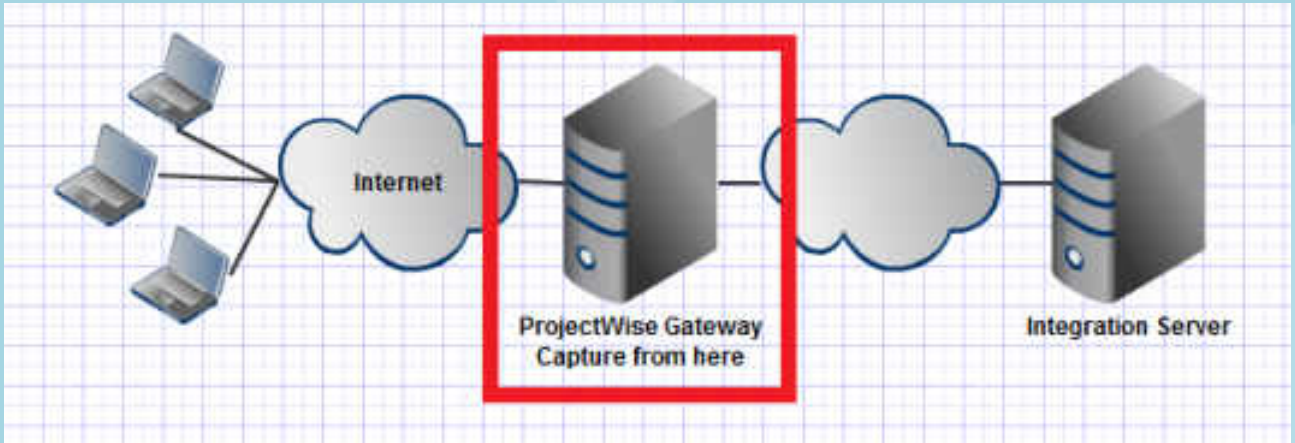


Answer

- Also got a capture on the server however we couldn't get it to upload to FTP or web based file sharing services, TCP connection would always reset
- After going a few rounds with users IT we were able to get captures from the edge of the server side network and found the issue was outside their firewall
- Users IT called the provider and they found a classic duplex mismatch between there device and the users firewall

2 - PW Gateway Connections issues

- Users having issues connecting / downloading files from internet facing gateway server
- Server is running ProjectWise Web Server and Gateway Server, both aren't working right
- Server in DMZ
- Server IP 192.227.137.48



Answer

- Seeing traffic from other servers on the subnet not targeted at the server we captured on
- Seeing a *LOT* of retransmits and malformed packets
- Turned out the switch was going bad.

3 – PW session getting closed

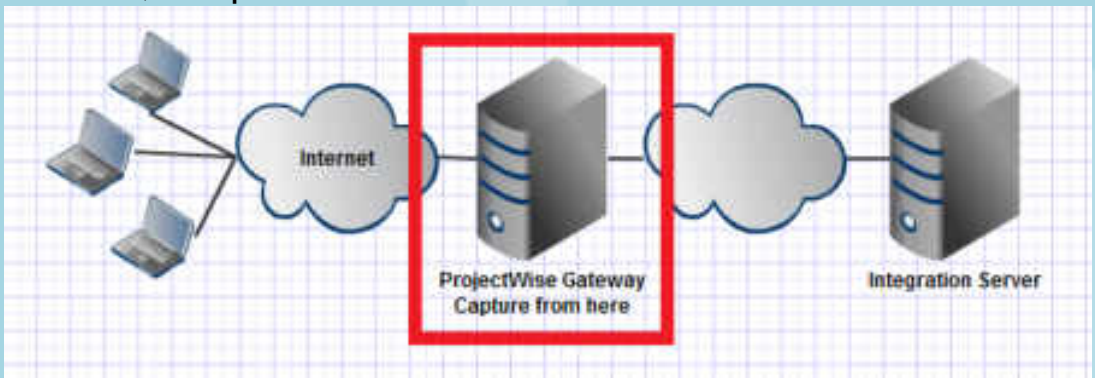
- User is able to log in to a 3rd party's ProjectWise server but there session gets 'randomly' closed out.
- Several organizations reporting this issue
- Log Snip

2010-04-07 16:18:54,201 pwise.ft - request sent, status = 0

2010-04-07 16:18:54,201 pwise.socket - socket_readFromSocket3: starting recv() bytes: 16 flags: 0x100

2010-04-07 16:19:51,155 pwise.socket - socket_getStatus: socket 724, timeout -1, select() returns 1

2010-04-07 16:19:51,155 pwise.socket - recv failed with status 10054

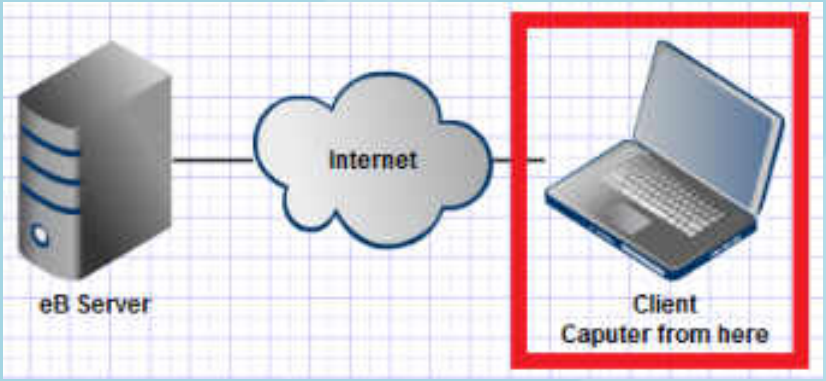


Answer

- User was getting ICMP fragmentation required messages back for full sized frame but based on the MSS at handshake the OS thought everything was OK so the frames were not fragmented causing a retransmits and the client to timeout and close the session
- Server side router was rebooted and the problem went away, router was replaced a few days later for good measure.

4 – eB Insight file upload fail

- User is trying to upload a file in to eB Insight and gets an error that ‘the connection is too unreliable’



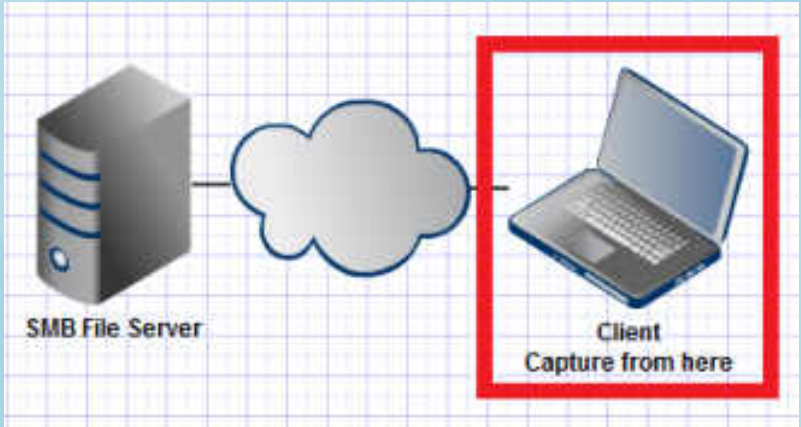
Answer

- The servers disk was full and the server was telling the client that but the client wasn't listening
- Freed up some space on the server and the issue was resolved.

OK, so maybe *sometimes* it is a software problem

5 – SMB mapped drive disconnect

- User reports there mapped network drive getting disconnect randomly which is causing design file corruption
- When trying to reconnect to the server they get an error 'Specified network name is no longer available'
- Capture from the client

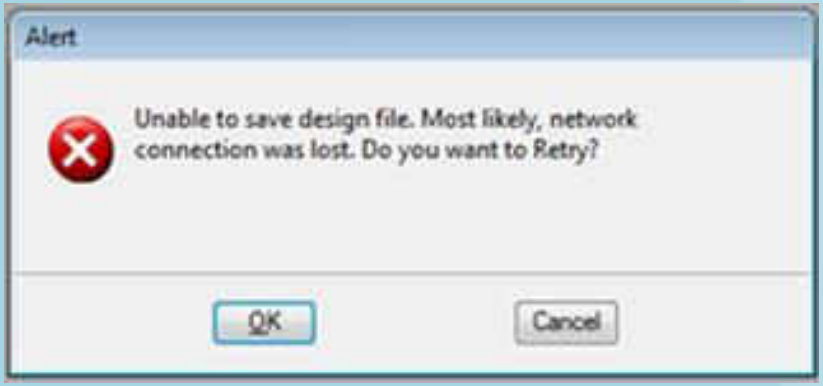


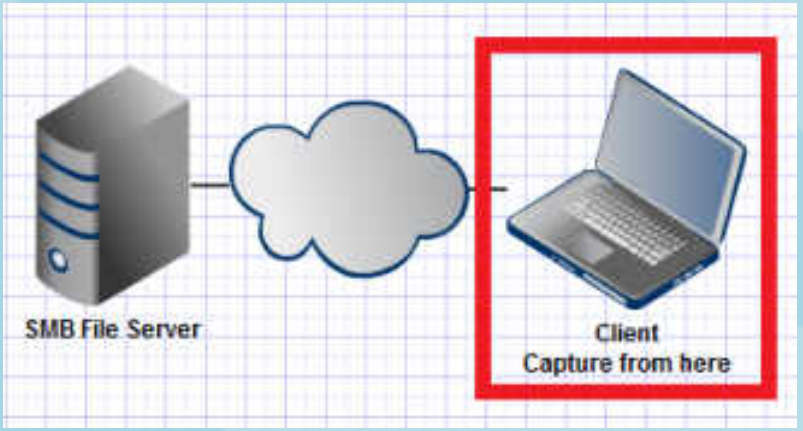
Answer

- After accusing the file of being the problem and then ruling that out found that Microsoft has a NUMBER of know issues in the SMB stack for server 2008 R2 and Windows 7
- Rollup KB
  - http://support.microsoft.com/kb/2775511
- Specific KB for this issue
  - http://support.microsoft.com/kb/2444328
- WARNING I have heard reports that some of the hotfixes cause problems for ArcGIS, test before applying

6 – SMB File save issue

- User getting messages that the file they have open for editing cant be saved
- Capture from the client



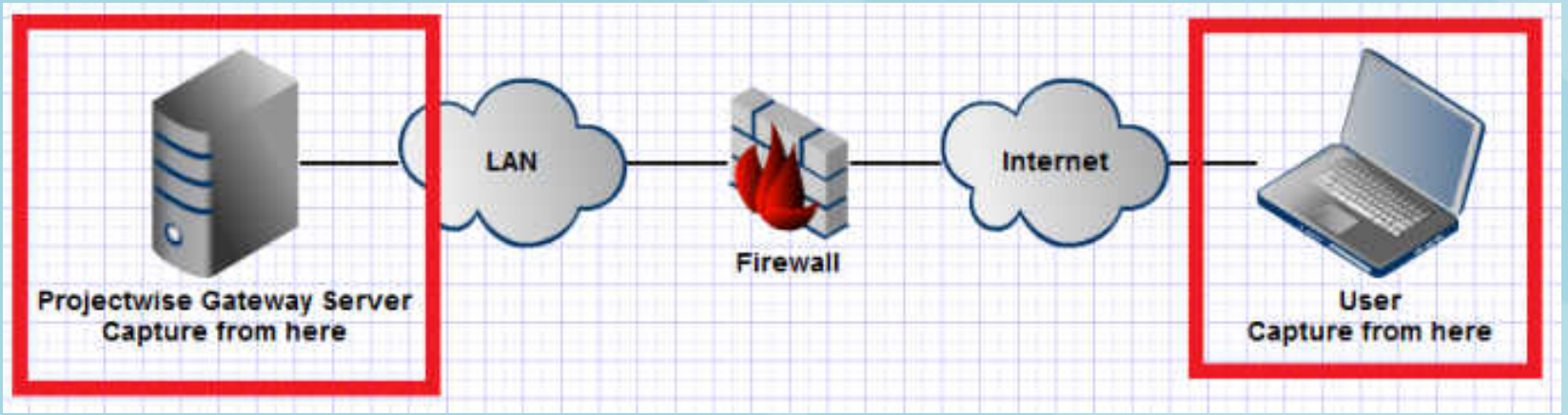


Answer

- Someone else opened the file for read so when the user went to write to the file they couldn't
- The application retried 8 times at 200ms intervals and then gave up
- User didn't see this problem before they went to server 2008 R2 / Win 7 (smb2), application had been tuned for smb1, lock timing changes in smb2 were 'causing the issue'
- Changes where made in the retry count of the application

7 - PW file download issues

- User is trying to download a file from ProjectWise across the internet and it always fails at the same point
- Most files work but a few do not



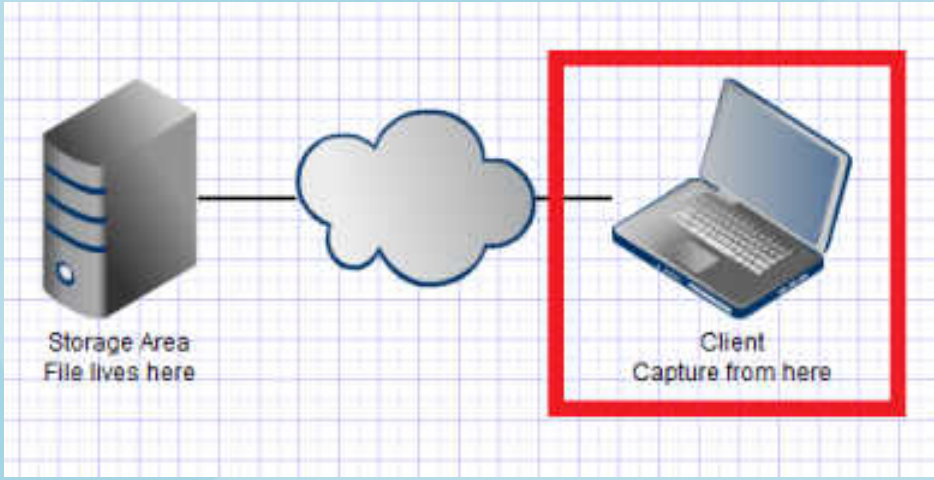
Answer

- There was a pattern in the file that was upsetting a device along the path
- NPING helped prove the ‘bad’ pattern and where about the packets were going missing
- Users IT didn’t believe the data so we ‘fixed’ the issue for the user by enabling SSL encryption on the gateway server

“This isn’t the traffic your looking for”

8 - PW client file download troubles

- User is having problems downloading files from ProjectWise, both errors and logs didn't make sense
- Wasn't sure what do to do but since 'downloading' is a network function we went fishing with WireShark



Answer

- In all the odd UDP traffic we see the word ‘LIME’ show up over and over
- This paired with the odd DNS traffic shows us the user is running LimeWire (or related P2P app)
- The P2P traffic was not the problem, the P2P app dropped a ‘bad’ dll on the system that took precedence over a windows dll and had a different implementation of a network function we were using

END of File - EOT

- If you can see this slide I have run out of content
- Questions / Comments
  - tim.poth@bentley.com