SHARKFEST '12

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
- Quick intro to ProjectWise
- 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
  - 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

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
    - Uses HTTP / SOAP to communicate

When 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,or bugs
- Wireshark helps us ‘prove’ where / what the problem is and get it fixed

About ProjectWise

- ProjectWise is a Client / Server application
- Uses a proprietary protocol on TCP Port 5800 (nothing to do with VNC)
- Uses DFT (Delta File Transfer) to speed up file transfer
- Each file transfer session starts a new TCP Connection using TCP port 5800
- Supports application specific “gateways” and “routing” - Server roles – Integration, Gateway, Caching, Web

About ProjectWise – Part 2

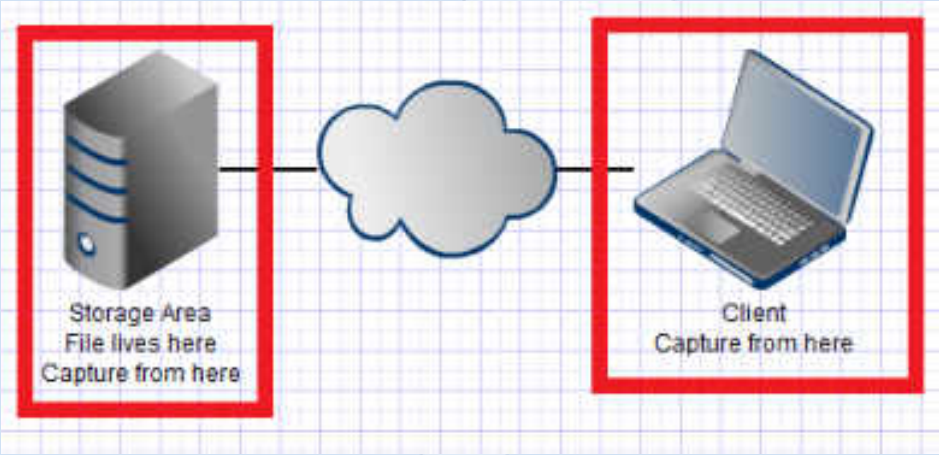
- The Web Server component is a ASPX page / ActiveX file transfer control over HTTP(S)
- A Datasource is a collection of folders / metadata hosted on a server, one server can have many Datasources, each Datasource can have many file storage locations

Last Notes

- This is a participation required session, speak up, ask questions

1 - Odd frame sizes

- In looking in to a file upload issue I found some very oddly sized frames

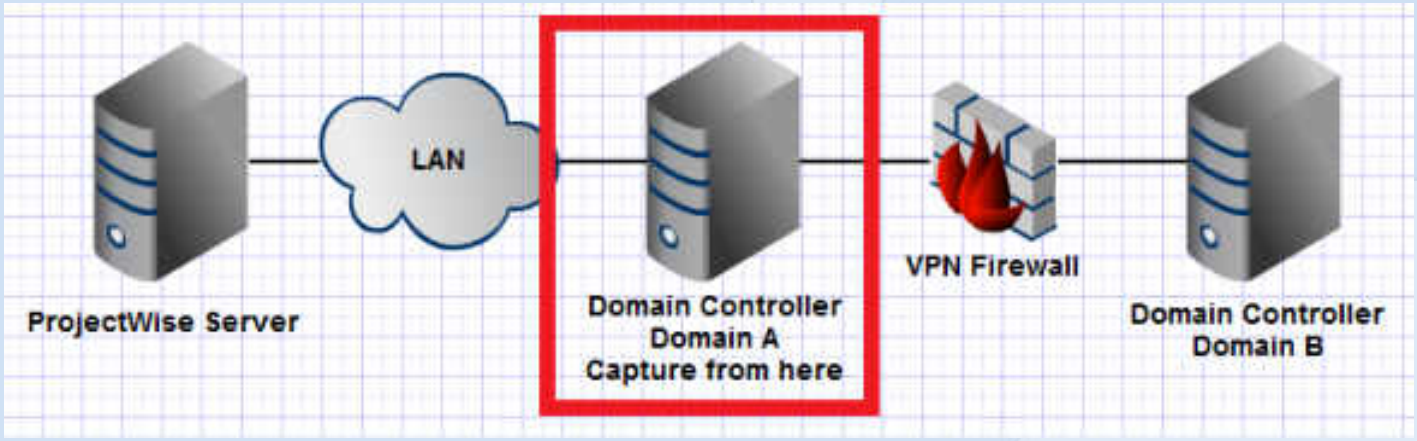


Answer

- Odd frame sizes had nothing to do with user issue
- Frame sizes were caused by a TCP offload option
  'Large Send Offload'
  AKA
  'Segmentation Offload'
  'TCP Segmentation Offload (TSO)'
  '[TCP] Multidata Transmit (MDT)'
  'TCP Large Send'

2 - PW DNS ‘issues’

- Unable to pull back domain controller list however lookup requests for specific servers works correctly
- PW server 172.29.29.132
  Domain A 172.29.29.135
  Domain B 172.27.128.5,172.27.69.10, 172.20.0.10

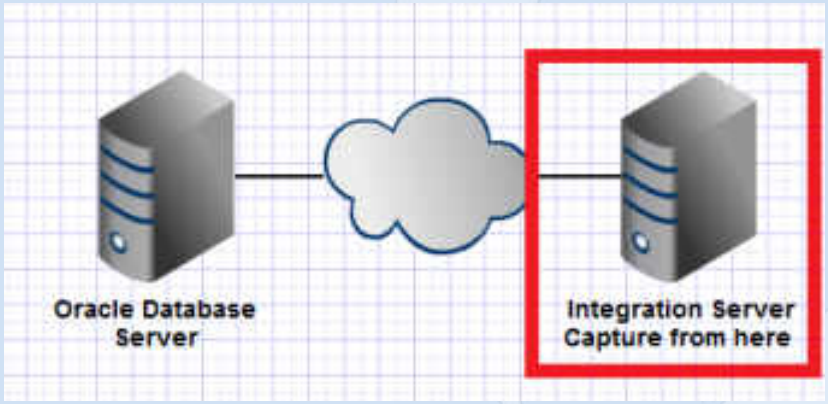


Answer

- The ‘Additional Records’ part of the request is a EDNS0 request (RFC 2671)
- The response was eaten by the firewall because it was larger than 512 bytes
  - EDNS0 supports responses larger than 512 bytes
- Users issue resolved by disabling EDNS0 on both sides of the firewall

3 - PW Database Performance issue

- User is complaining application slowness, logs show delays getting data back from the Oracle database.
- Database is connected to app server via a WAN link so there is concern there is a network bottleneck

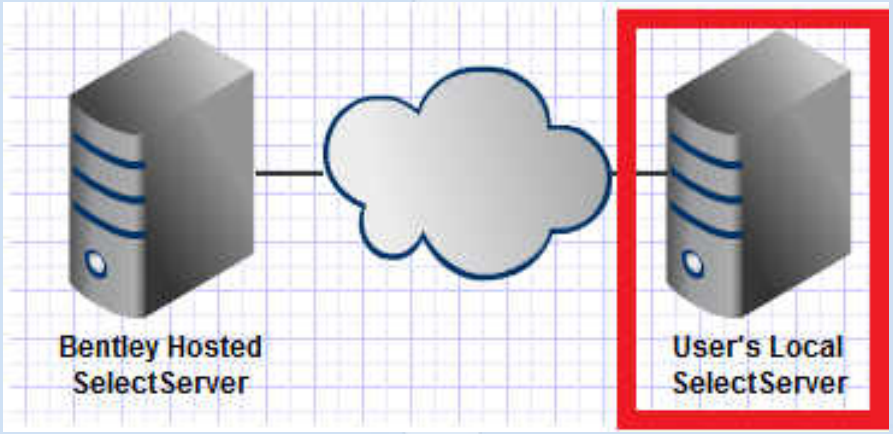


Answer

- The performance issue was caused by the amount of data in the database and the way it was laid out on the servers disks, there was no problem with the WAN link
- The small packets were corrected with a few settings changes in Oracle to better utilize the available bandwidth.

4 - SS Usage submission failing

- SelectServer is trying to post its usages to Bentley and failing



Answer

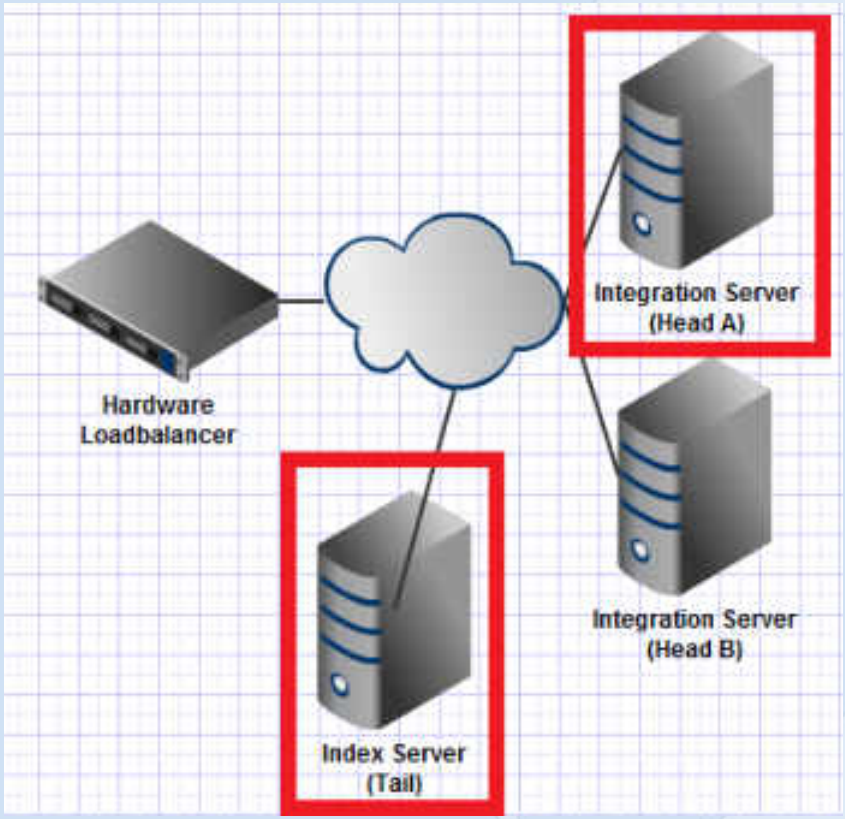
- In this case we can clearly see everything we try is met with a 503 service unavailable
- We can make a good guess it isn't Bentley's servers because of how quick the response comes back and the fact that there is a user name in the error, Bentley wouldn't know this
- Users IT resolved with out providing detail

5 - PW socket error

- When connecting to the cluster from the index server (tail) using ProjectWise Client user gets a socket error, All other traffic seems fine
- User has 2 integration servers (head) in a NLB cluster using a hardware load balancer
- To create the capture all traffic was forced over to 1 head server
  - The head servers is 192.168.118.151
  - Tail is 192.168.118.154
  - Load balancer cluster IP is 10.190.22.247

5 - PW socket error

- Network layout

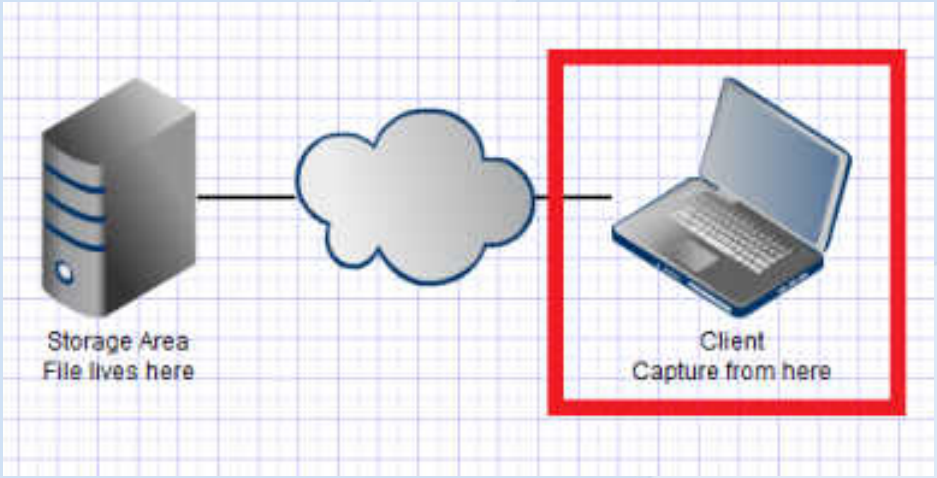


Answer

- Because Head and Tail are on the same network they can talk directly with each other so when the Load Balancer passes the traffic along the Head makes a direct response back to the tail
- Because the clients are not on the same network the Server has to talk thought its gateway (the Load Balancer) and things work better.
- Users IT enabled NAT on the Load Balancer to resolve the issue

6 - PW file download fail

- User is trying to download 'BSI700-A0101-PumpHouse.dgn' from ProjectWise
- The download seems to hangs at the end and then fails with a error
- There is nothing of use in the log files

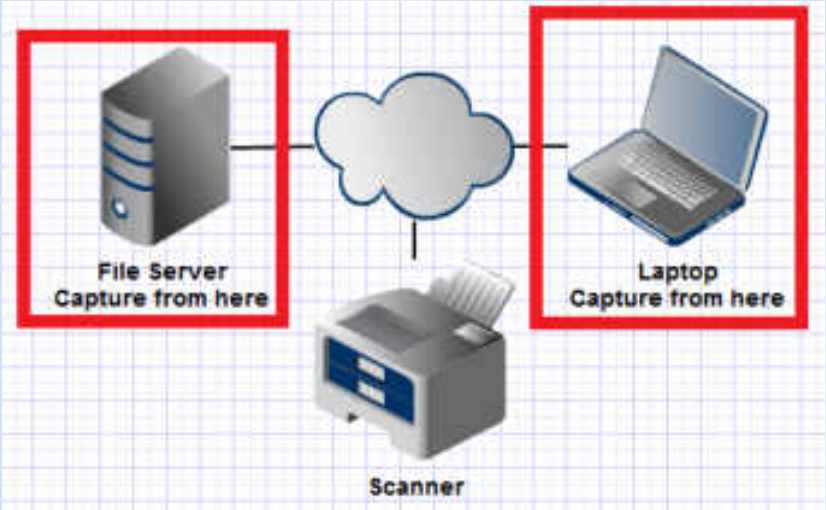


Answer

- When we download a file with DFT we copy the original file to a temp file, apply the changes, delete the original file and rename the temp file to the original
- In this case the delete command was reported as ‘completed’ however it wasn’t
- When we tried to rename temp file to the original name we got an error
- ProjectWise Client tried a few times and gave up
- Users IT resolved with out providing detail

7 – SMB Cant scan to new server

- Small office just put in a new file server (2008 r2) and when they set there (old) scanner to save the files to a share on the server they get a error.
- Created a capture on the server of the scanner failing and then a capture from a laptop showing that the share can be accessed

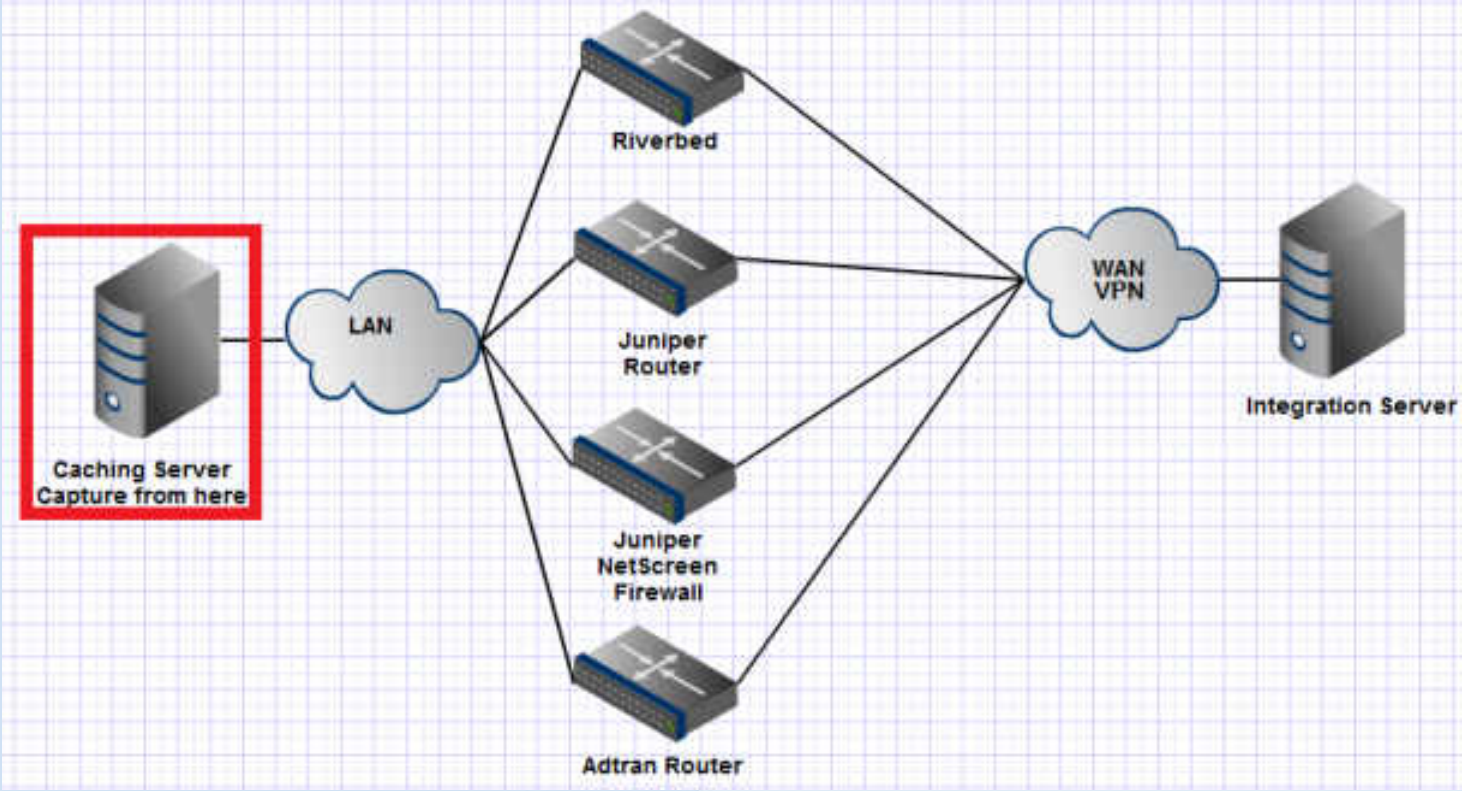


Answer

- Because this server is a domain controller and server 2008 r2 the default security settings had changed from the old 2003 server.
- The group policy setting ‘Microsoft network server: Digitally sign communications (always)’ was causing the issue
- Because a firmware update wasn’t available we disabled the setting in the group policy

8 - PW Random connection issues

- Users at one site randomly cant connect to integration server via a Caching Server



Answer

- Looking at a good and bad streams, network traffic takes much different paths
- The ICMP redirects sent new connections off a different direction
- User IT resolved the issue by making configuration changes to prevent the client from getting the redirects

END of File - EOT

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