Wireshark Developer and User Conference

Using WireShark to support the Application

June 16, 2011

Tim Poth

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

SHARKFEST '11

Stanford University

June 13-16, 2011

Agenda

- Quick intro to Bentley Systems, Inc
- How the Priority Response Team (PRT), uses Wireshark to support our applications
- Quick intro to ProjectWise and SelectServer
- Look at 13 different user problems and how Wireshark help get the issue resolved

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

- PRT primarily supports 2 applications with Wireshark; ProjectWise and SelectServer
- ProjectWise – we already introduced this
- SelectServer – licensing server, records product usage

What we use Wireshark for

- 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 it runs in to
- 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) in newer versions to speed up file transfer
- Each file transfer starts a new TCP Connection (starting to reuse file transfer connections in latest version)
- 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

About SelectServer

- IIS / .NET application that processes / records product usages in a database
- Usage data is communicated via SOAP over HTTP(S)
- Has a reports component that publishes usage data via aspx page
- Bentley hosts a public instance on the internet, clients can also deploy a locally instance. Local servers send usage data to public instance

Last Notes

- If you see an ip address 127. consider it a valid IP address, I changed some registered IP address
- This is a participation required session, speak up, ask questions

1 - PW ‘Long’ Client launch

- User is complaining about how long it takes for ProjectWise to open and display datasources
- The capture is from the Gateway Server the user client was pointing at on startup. Log snip is from the same box

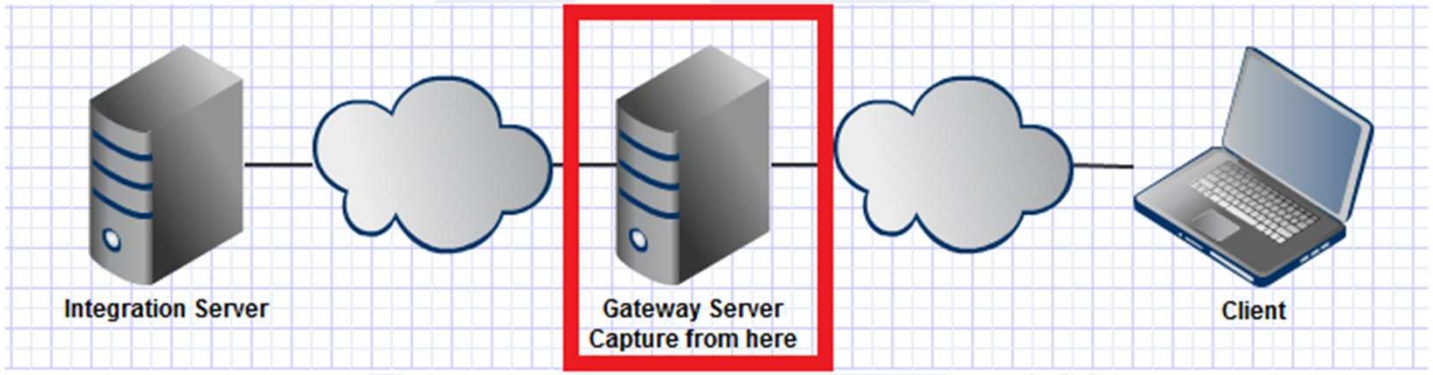
2008-10-22 16:25:45,264 INFO [3644] pwise.request - Start Request < NameServer List > <4601,17> #1 addr: 127.77.3.29 socket: 1508 session: 0x44fe4a0

2008-10-22 16:25:52,077 DEBUG [3644] pwise.socket - socket_sendToSocket3: starting send() bytes: 2086 flags: 0

2008-10-22 16:25:52,077 DEBUG [3644] pwise.socket - socket_sendToSocket3: send() done, result = 2086

1 - PW ‘Long’ Client launch

- Network layout

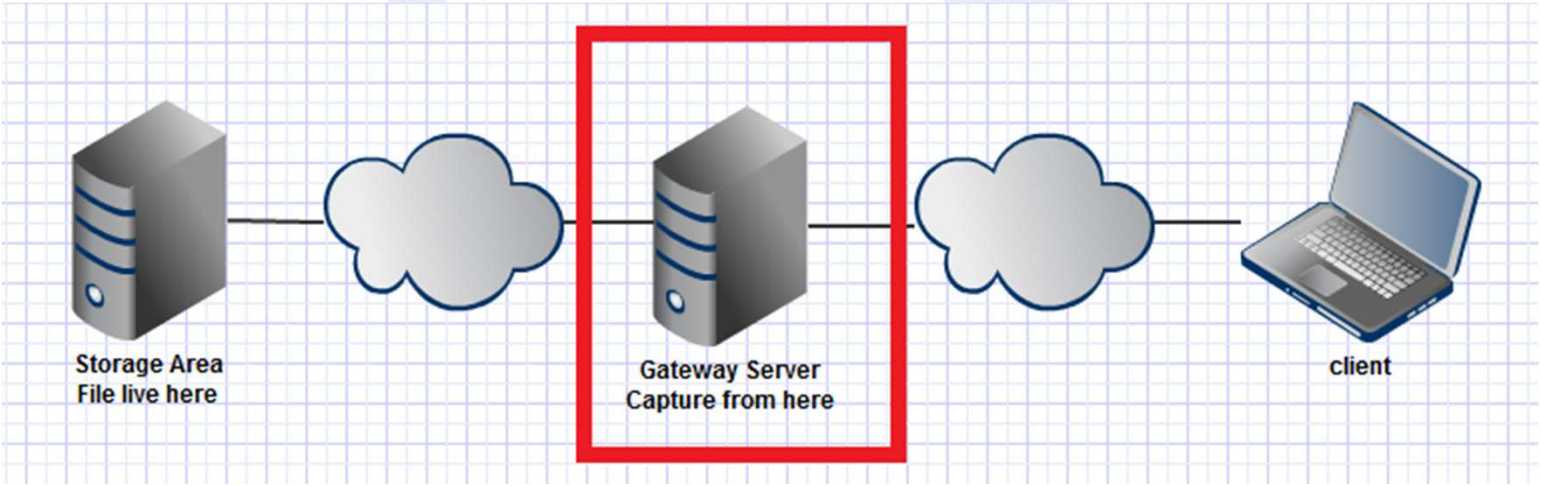


Answer

- ProjectWise wanted to resolve the name of a few of their servers based on a configuration file and asked Windows
- DNS couldn't resolve the names so Windows started NBNS (NetBios Name Service) broadcasts
- Lag was due to waiting for NBNS time out
- User IT added servers to there DNS zone which resolved the issue

2 - PW Client slow file download

- User is seeing delays downloading files through a ProjectWise Gateway server.
- Log files didn't show anything useful
- Capture from the Gateway Server

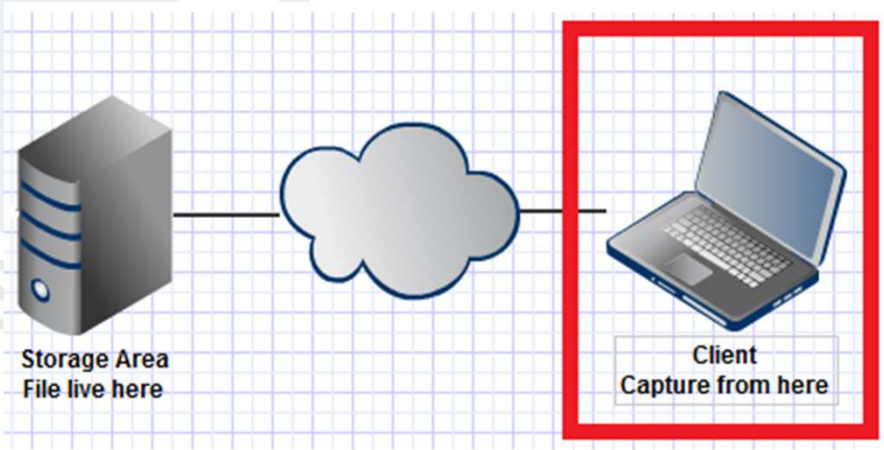


Answer

- ProjectWise was requesting a reverse DNS lookup which ran in to 2 problems
  - The reverse lookup zone is not setup / does not have this host listed in it
  - The DNS server is taking WAY to long to respond back
- User IT found the Gateway Server was pointing at the wrong set of DNS servers which caused the delay and the failed lookup

3 - 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
- Captured from Client

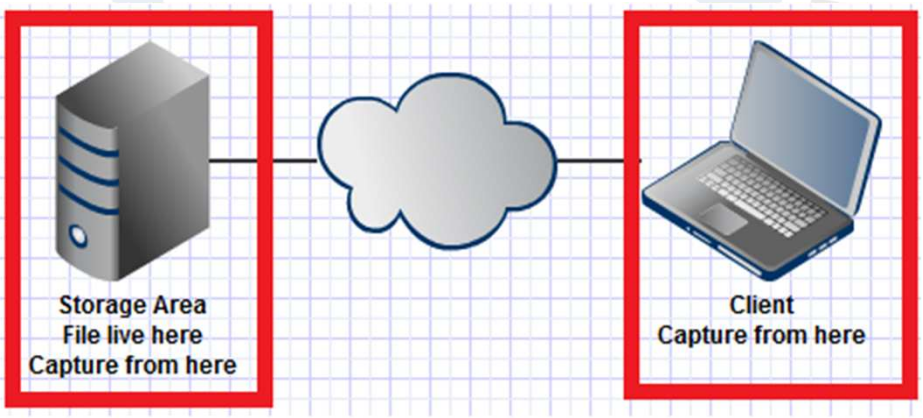


Answer

- 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

4 - PW File Download

- User is trying to download a file from ProjectWise which causes PWC to hang
- PWC logs make it look like client is waiting on the server.
- Capture from Client and Server



Answer

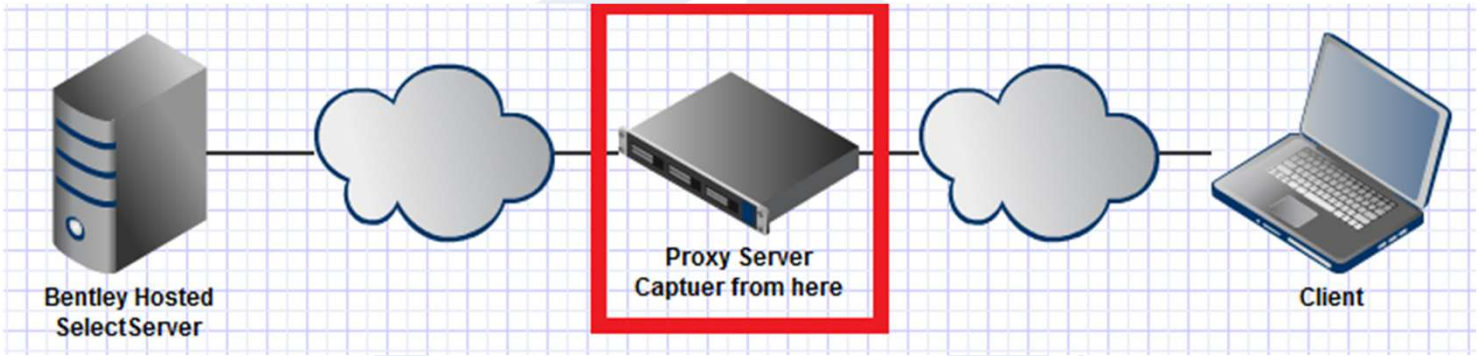
- The server and the client are able to talk up until the point were the file transfer start
- In looking at the server capture we can see that once the file transfer starts the server gets ICMP type 3 code 3 responses back from the router
- Something about the transfer upset the firewall
- Users IT resolved configuration issue on firewall

5 - SS Summary Report failure

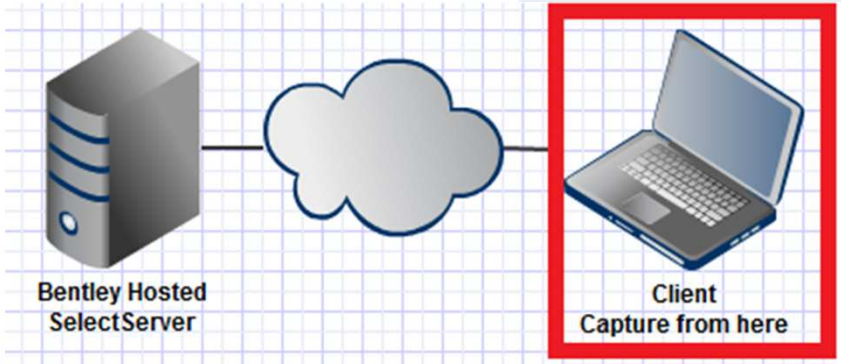
- User is trying to run a Summary Report off the SelectServer hosted by Bentley, gets a error back from their proxy server
- Capture from their proxy server and stopped as soon as the error came up
- The working example file is a capture of the same procedure which completed without error from my computer on Bentley's network

5 - SS Summary Report failure

- Network Layout
  - Not working



  - Working

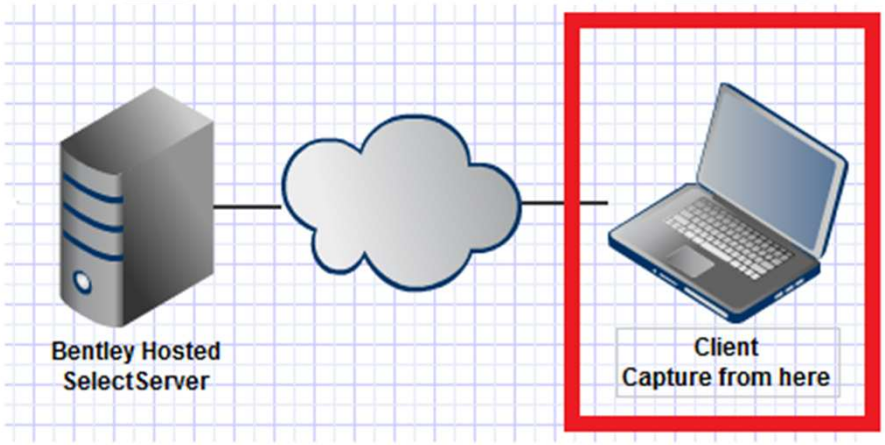


Answer

- Once we track down the good and bad requests we can see that the proxy is injecting keep alive data in to the cookie causing it to be malformed
- This causes the IPS protecting the server to reject the cookie – kill the session
- Users IT resolved with patch from proxy vender

6 - SS Licenses download fail

- User is trying to get a licenses from Bentley's SelectServer and is getting a message that the licenses is Invalid
- Capture was taken from the Client

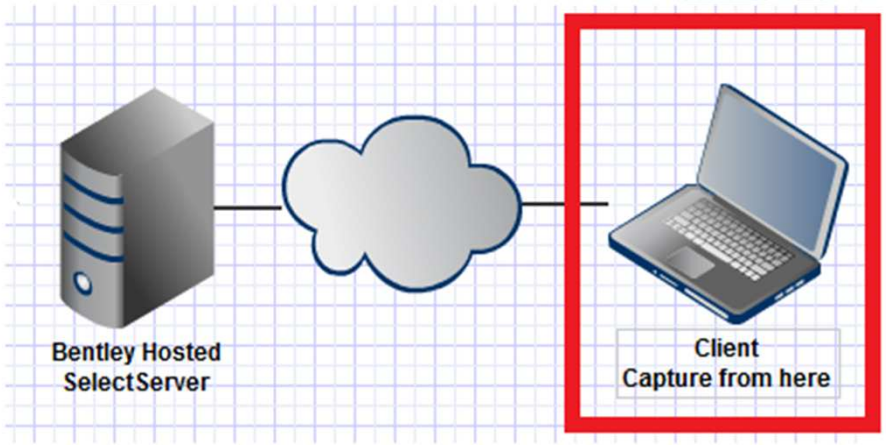


Answer

- The working replies seem to be coming from Firewall A but when the connect gets shutdown (RST / ACK) the reply comes from Firewall B based on the MAC address
- Client computer was failing back and forth between the 2 firewalls at random
- Users IT resolved issue with out providing any details

7-SS License usage upload fails

- User is trying to push some data to the Bentley SelectServer and it fails with an error
- Capture from Client

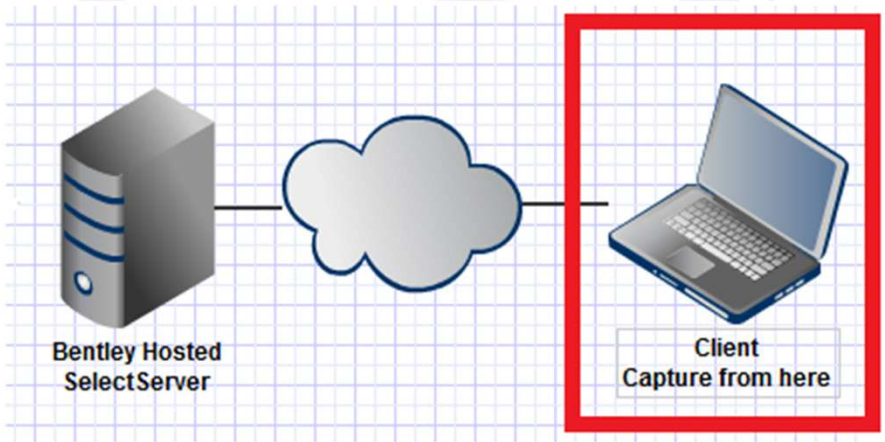


Answer

- We seem to get a 417 response for each request we make
- In looking at the HTML we can see the server is a SQUID proxy and the request is flagged as a ‘Invalid Request’
- This is a documented ‘issue’ with SQUID
- Users IT upgrade SQUID to resolve issue

8 - SS Licenses management tool fails

- User is trying to use the license management tool to get a license from SelectServer but it is failing
- Capture from client

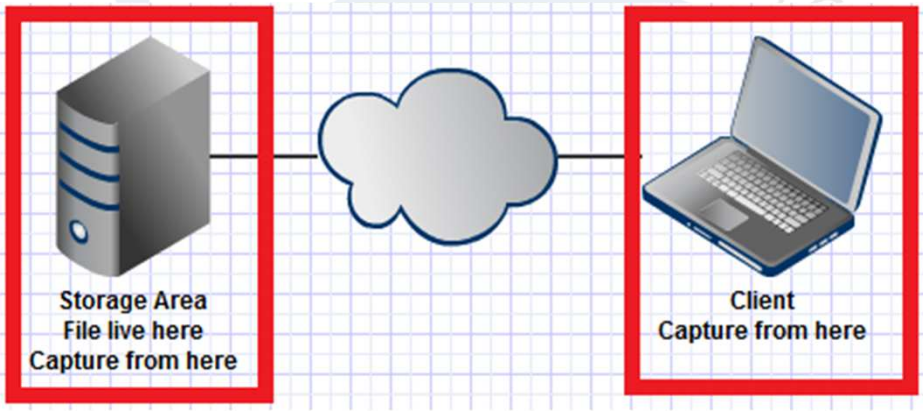


Answer

- At first it looks like a proxy authentication issue but if you look a bit more carefully (note the times) the request times out after 30 sec
- Users IT resolved with out providing detail

9 - PW File upload hang

- User is having problems uploading files to ProjectWise, the transfers keep hanging
- Logs didn't show anything useful so we got a WireShark capture
- Capture from Client and Server

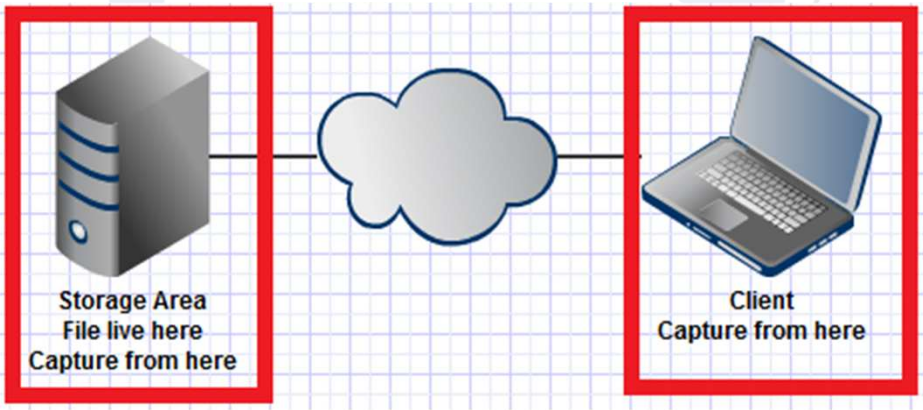


Answer

- What we've got here is a failure to communicate
- Traffic drops out in the middle of the communication
- Client gets all the servers Dup ACKs but the server never gets the retransmits
- Users IT resolved with out providing detail

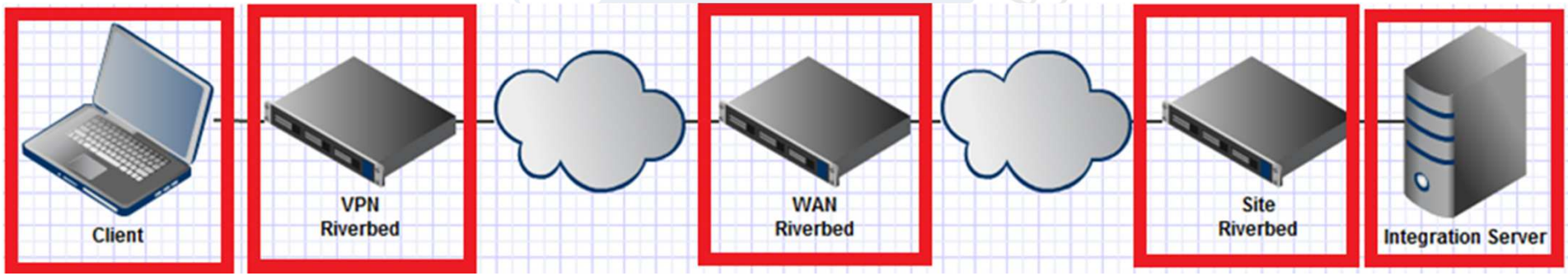
10 - PW login failure

- When the user tries to login to ProjectWise it would sometimes fail with an error
- There are several datasources and not all have a problem, some are worse than others.



10 - PW login failure + a little more

- Ran a capture on the client that showed some interesting things so we took another capture from the client, 3 Riverbed devices and a frequent problem server
- Tried until we failed
- Network layout



Answer

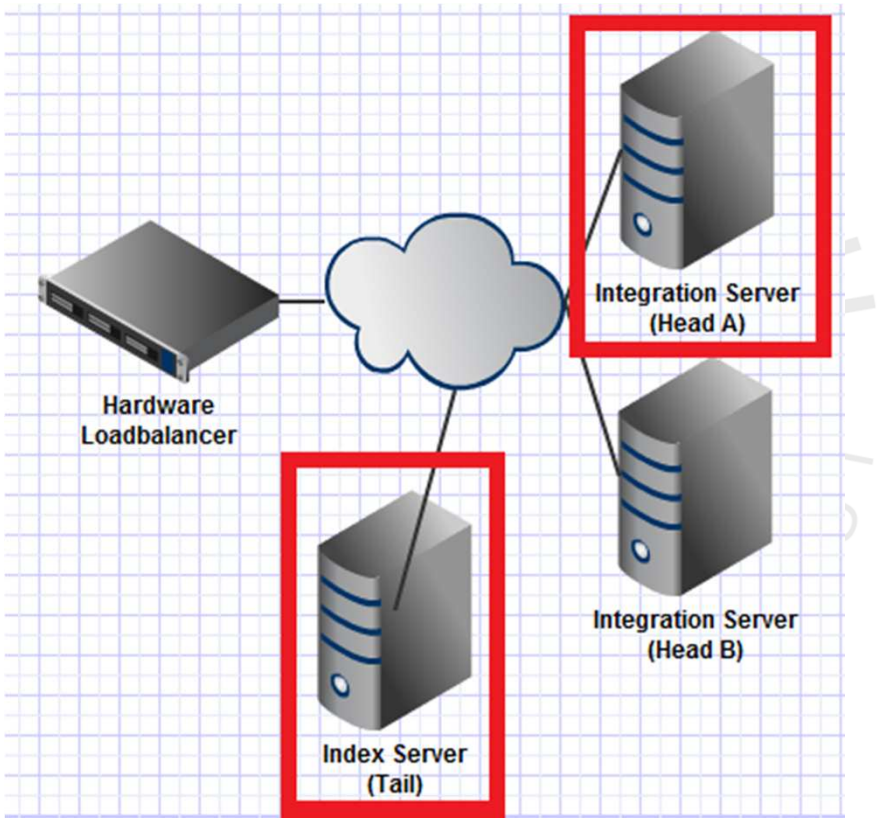
- Much like example 9 we have a breakdown in communications however it this case we got a few more captures showing what leg of the link had the problem
- From this the users network team (eventually) found they had a async route setup with out the corresponding rules on the firewall
- Randomness of the issue resulted for network load
- Users network team added rules to the secondary firewall which resolved the issue

11 - PW socket error

- User has 2 integration (head) servers in a NLB cluster using a hardware load balancer
- When connecting to the cluster from the index server (tail) using ProjectWise Client they get a socket error
- 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
- Other users on the network work fine, this just effects traffic between the heads and tail
- Capture from head and tail.

11 - PW socket error

- Network layout

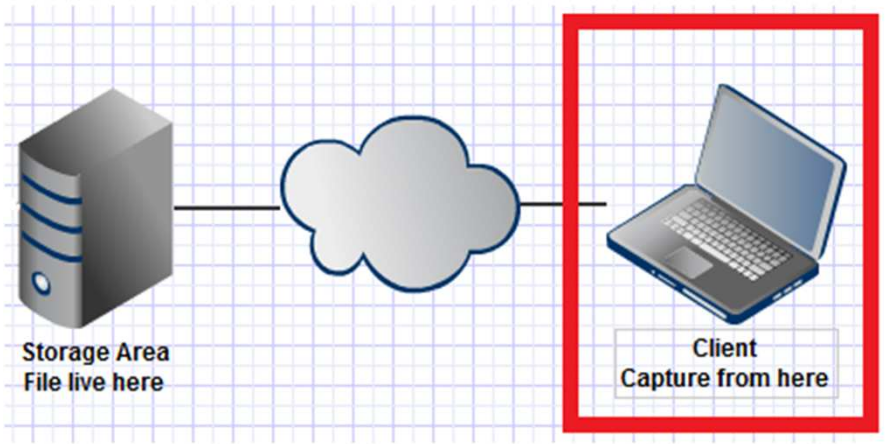


Answer

- 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 just makes a direct response
- 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

12 - 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
- Capture from Client

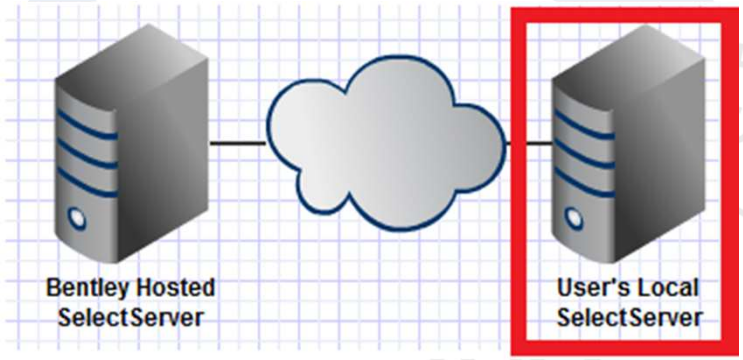


Answer

- 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
- We tried a few times and gave up
- Users IT resolved with out providing detail

13 - SS Usage submission failing

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



Answer

- In this case we can clearly see everything we try is met with a 503 service unavailable
- We can make the 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

END of File - EOT

- If you can see this slide I have run out of content