SHARKFEST '12

Wireshark Developer and User Conference

WireShark Case Studies

Tim Poth

Senior Priority Response Analyst

Bentley Systems, Inc.

tim.poth@bentley.com

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
- Primarily supports 2 applications with Wireshark: ProjectWise and SelectServer
  - SelectServer – licensing server, records product usage
    - Uses HTTP / SOAP to communicate

When do we use Wireshark

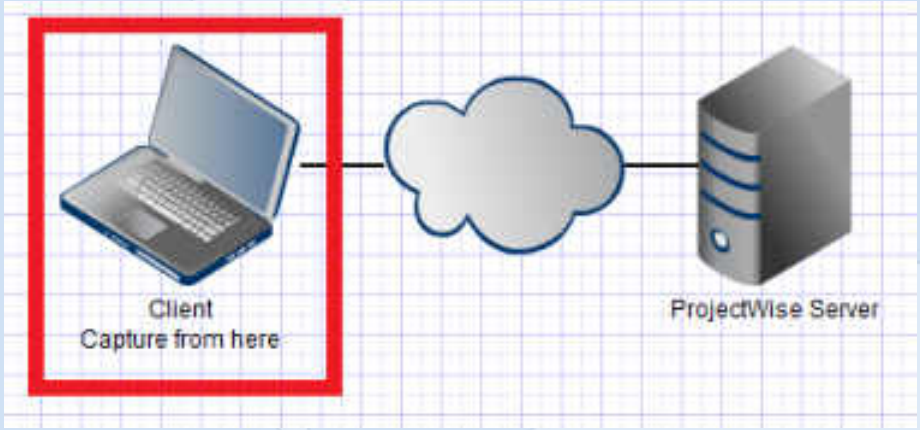
- When a company has a problem with our applications we often have to work with the end user or application admin, not a network admin
- We use Wireshark to understand how our application is behaving on their network and to track down obstacles preventing it from working correctly
- Sometimes we find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

Case One – The Problem

- We had a large organization seeing random failures trying to login to ProjectWise
- This organization has 7 different integration servers in 7 different locations around the United States
- Users are connecting in from dozens of site, all seeing the issue.
- There are several datasources and not all have a problem, but some are worse than others.

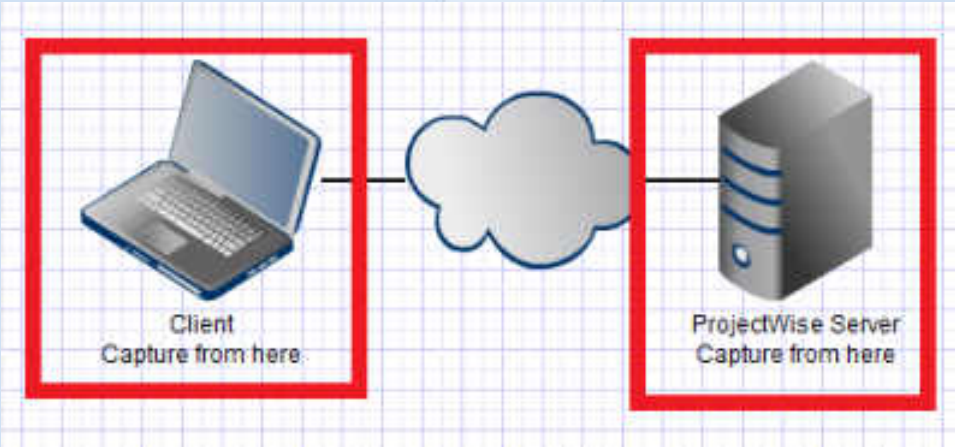
Case One – Round One

- First step was to look at the client logs. In the logs we found the connection was ‘hanging’ at the application handshake phase and then erroring out.
- Ran Wireshark on the client to see what this ‘hang’ was all about



Case One – Round Two

- We see the 3-way handshake completed but why two syn/ack packets?
- The hang is caused by the retransmissions so what does the server see?



Case One – Round Three

- The server shows the 3-way handshake without the second syn/ack
- There are some extra frames in between the handshake and the retransmits
- The important point is the server is sending a reply to the clients request SO someone in between must be eating them, but who?

Case One – Narrowing the scope

- The VPN Riverbed capture looks like the client so its not in between those two.
- The WAN Riverbed capture looks like the Client and the VPN Riverbed (except the missing syn/ack) so it's not between the client and WAN
- The Site Riverbed looks like the server! So the issue must be on or between the Site and WAN Riverbed devices

Case One - Answers

- The users network team (eventually) found they had second link setup between the Server Site and the Company Hub BUT didn't have corresponding rules on the firewall
  - async routing isn't bad but can cause confusion
- Randomness of the issue was the resulted of network load; when the load got high enough traffic would spill over to the second link and get blocked
- Users network team added rules to the secondary firewall, which resolved the issue

Case One – Lessons

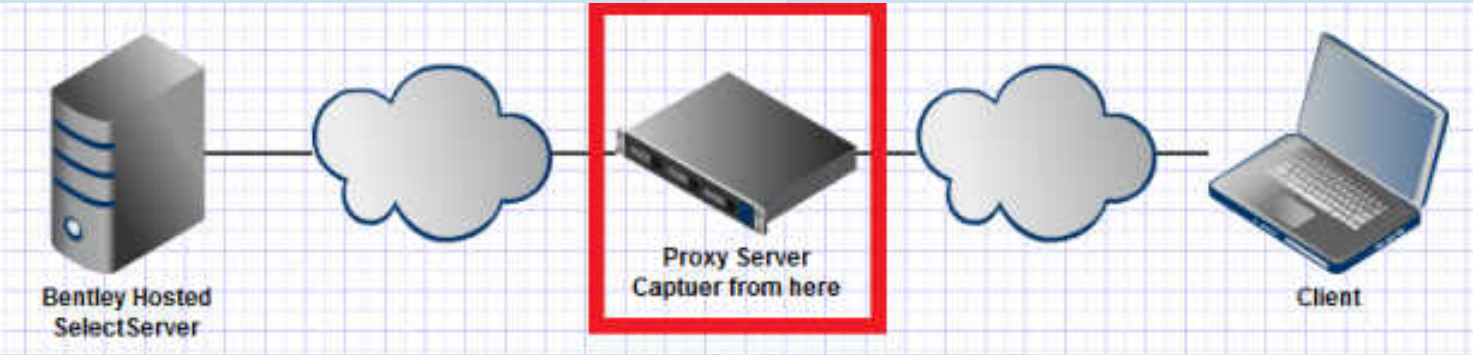
- Doesn't matter how big the network is, cut it up in to chunks until you close in on the issue
- This issue was seen accessing server at several different locations; we picked one and worked it. Don't ignore the other sites but don't get hung-up on them; you can only do so much at once
- All the problem sites were setup the same. Stander configs can lead to standard errors

Case Two – The Problem

- User is trying to run a Summary Report off the SelectServer hosted by Bentley but is getting a error back from their proxy server that Bentley killed the connection
- No one else is having an issue running reports from Bentley's server but the user can find no fault with their proxy and has no issue with any other site

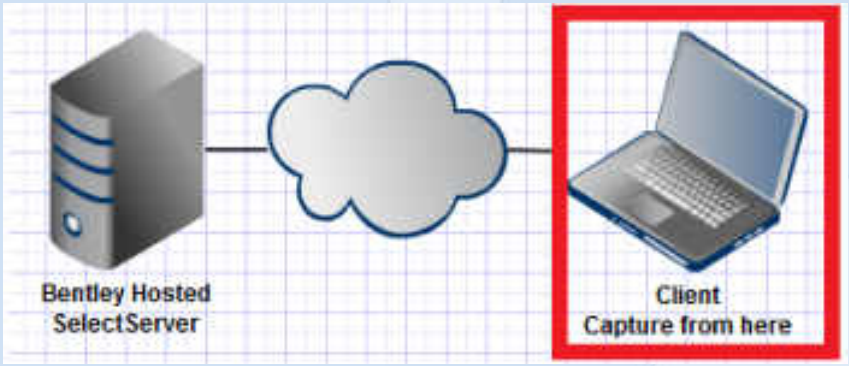
Case Two – Round One

- Created a capture from their proxy server to see how things were going with Bentley. We didn't capture from his workstation because all we would see is the proxy complaining about us



Case Two – Round Two

- We see the reset came back from Bentley, so I guess the proxy isn't lying, but there must be a reason it's only this user having a problem
- Maybe there's something wrong with their request. What does a good request look like?
- Create a capture from my system to get a baseline



Case Two – Proving our point

- So we found some text in our cookie that looks like it was injected but no other site has a problem with this so how do we prove it out?
- We crafted our own http request and, using wget, sent it to the Bentley server, and the request was rejected with a reset
- We then got together with our firewall guys to tell us why, and after a few tests we found the request was failing a cookie validation rule

Case Two - Answers

- With all the data on hand we went back to the user and laid out our case
- They got in contact with Blue Coat who agreed they shouldn't be injecting things in to cookies like that and issued a patch

Case Two – Lessons

- Just because no one else sees an issue doesn't mean your firewall isn't telling this client to go away
- When something doesn't make sense focus on the differences between a good and bad case
- Look for tools that let you build a test case

END of File - EOT

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