# CIFS/SMB2
# Deep-Dive Report

## Created for “Sample Report”

Jun 25th 2013 – Jul 8th 2013

Written by: Esben Laursen – Hawk-Eye – el@hawk-eye.eu

# Contents

# Introduction

## *Preface*

This report takes a deep-dive into the CIFS/SMB2 protocol optimization on Steelheads within your estate. This report includes an executive summary as well as details of the error profiles in the network. Additionally we provide recommendations on configuration changes, and best practice advice in order to facilitate fast identification of the Steelheads, servers or clients generating problems and the causes. This will enable the Steelhead administrator to conduct reconfiguration or further troubleshooting quickly and easily, saving time, money and resources.

## *Executive Summary*

We have seen many problems with the CIFS/SMB2 protocol optimization, we have detected an error rate of >55% over the last 14 days. We have seen more than 410.000 sampled sessions with reduced optimization performance. This means that more than 410,000 sampled sessions have not been fully optimized, affecting both network performance and user experience.

In general there are 2 issues; a) SMB2 is not enabled and b) SMB-signing is required

a) SMB2 is easily remedied as all Steelheads supports SMB2 the configuration needs to be changed so this feature is enabled.

b) Two common issues with SMB-signing are that it has not been enabled or it has been configured incorrectly. As the Steelheads are on a recent version of RiOS that supports SMB signing in transparent mode, it is highly recommended to join the all Steelheads as a Read-Only Domain Controller (RODC) and optimize it in transparent mode.

   If company security policy allows it, an alternative to joining the Steelheads as a RODC is lowering the SMB signing level to “enabled” from “required”. If this is implemented, there is no need to make additional configuration changes on the Steelheads as SMB signing will no longer be in use in the network.

## *How sessions are counted*

### Sampled vs. aggregated dataset

“Sampled dataset” means we collect data ~~on~~ at fixed time intervals, only retaining the content of the register at the time of collection.

“Aggregated dataset” means that the device is retaining all data, and when collection takes place we are passed the aggregated values accumulated since the previous collection took place.

Which is the more precise method?   “Aggregated” is considered a more valid sample, however if the time period is long enough and enough samples are collected, both methods will deliver similar results and conclusions.

### How we collect data and analyse

We collect data using different methods; the primary method used for this report utilises the CLI (Command Line Interface) on the Steelhead. There is no detailed connection history of closed sessions on the Steelhead at the time data is collected; we only have a sampled dataset for this metric.

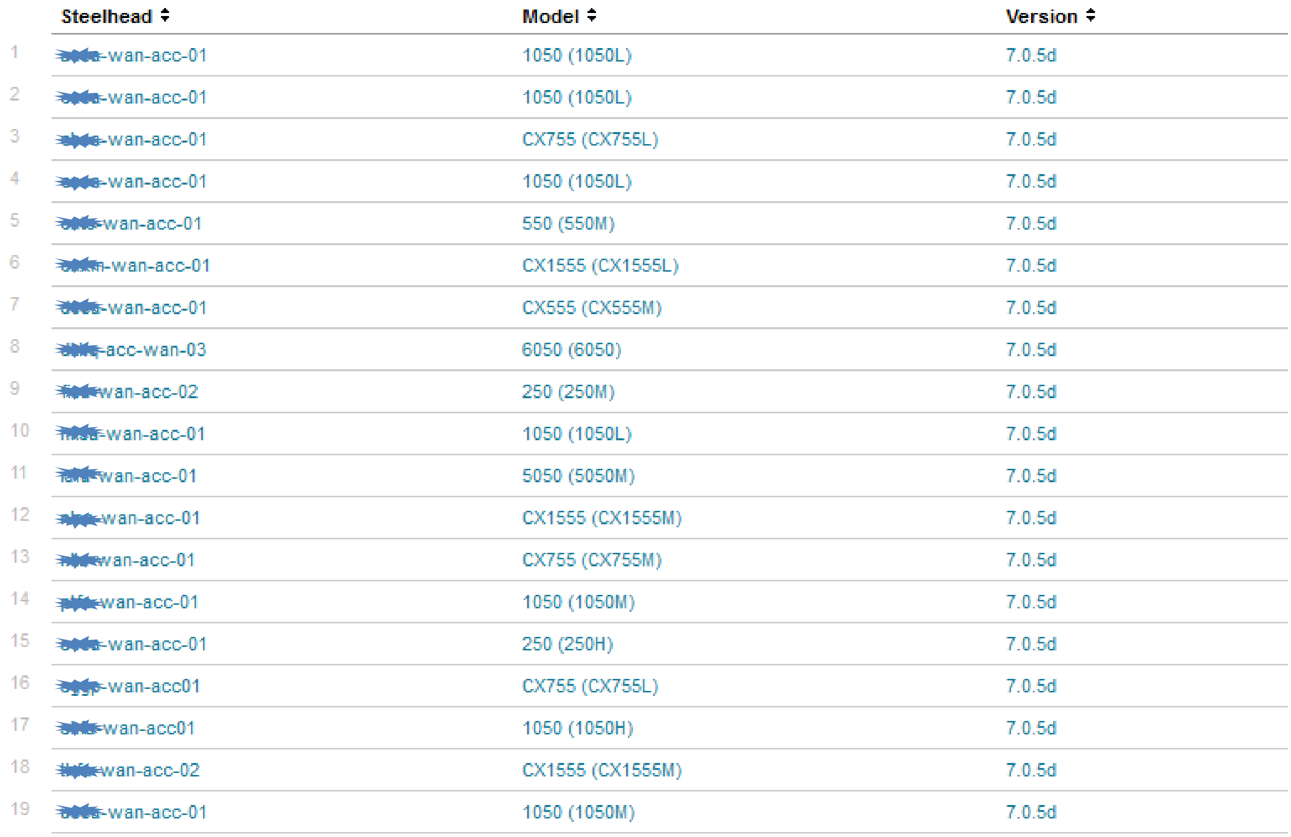
This means that approximately every 5 minute we log on to the Steelhead and collect a sample of the “Current Connection Report” and analyse it. This also means that if a session is both opened and closed in between sample data being collected it will not be detected. Conversely this means that if the session is persistent, for example one lasting an hour, it will be counted 12 times in a 60 minute period.

The disadvantage of a sampled dataset is that we only see traffic at the time we look (once every 5 minute) and we do not detect data outside this. This is not the most comprehensive method, but it is the only one available to us, and over time it gets more precise meaning the output and conclusions become more robust.

We may also, depending on the result extract information from the logs collected (syslog) and/or from SNMP and include this in the report.

# Steelheads in Scope

This is a list of Steelhead that has been analyzed

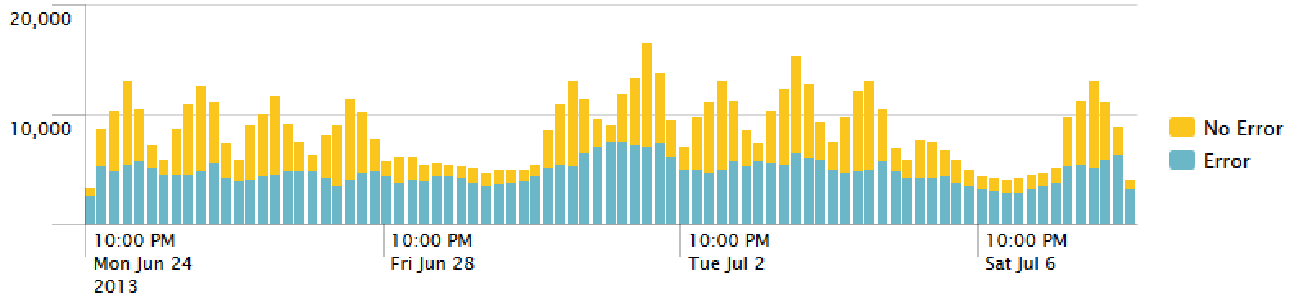


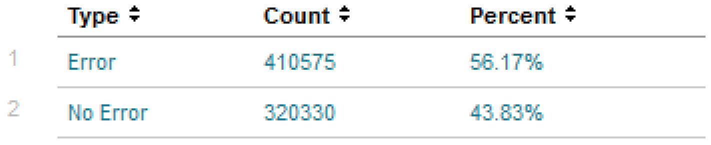
| | Steelhead ⬍ | Model ⬍ | Version ⬍ |
|---|---|---|---|
| 1 | [redacted]-wan-acc-01 | 1050 (1050L) | 7.0.5d |
| 2 | [redacted]-wan-acc-01 | 1050 (1050L) | 7.0.5d |
| 3 | [redacted]-wan-acc-01 | CX755 (CX755L) | 7.0.5d |
| 4 | [redacted]-wan-acc-01 | 1050 (1050L) | 7.0.5d |
| 5 | [redacted]wan-acc-01 | 550 (550M) | 7.0.5d |
| 6 | [redacted]-wan-acc-01 | CX1555 (CX1555L) | 7.0.5d |
| 7 | [redacted]-wan-acc-01 | CX555 (CX555M) | 7.0.5d |
| 8 | [redacted]-acc-wan-03 | 6050 (6050) | 7.0.5d |
| 9 | [redacted]wan-acc-02 | 250 (250M) | 7.0.5d |
| 10 | [redacted]-wan-acc-01 | 1050 (1050L) | 7.0.5d |
| 11 | [redacted]wan-acc-01 | 5050 (5050M) | 7.0.5d |
| 12 | [redacted]-wan-acc-01 | CX1555 (CX1555M) | 7.0.5d |
| 13 | [redacted]wan-acc-01 | CX755 (CX755M) | 7.0.5d |
| 14 | [redacted]wan-acc-01 | 1050 (1050M) | 7.0.5d |
| 15 | [redacted]-wan-acc-01 | 250 (250H) | 7.0.5d |
| 16 | [redacted]-wan-acc01 | CX755 (CX755L) | 7.0.5d |
| 17 | [redacted]wan-acc01 | 1050 (1050H) | 7.0.5d |
| 18 | [redacted]wan-acc-02 | CX1555 (CX1555M) | 7.0.5d |
| 19 | [redacted]-wan-acc-01 | 1050 (1050M) | 7.0.5d |

## Optimization Errors vs. No Errors

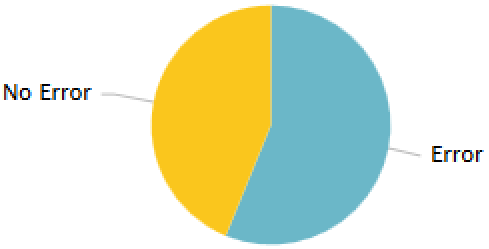
In this section we have analyzed how many errors were logged, comparing  it to the number of sessions optimized with no errors. Please note that an error is not a session that is broken from the user perspective it's an error in the optimization.

When we see optimization errors, it means the Steelhead cannot perform layer7 optimization, but is capable of bandwidth optimization only. Without Layer 7 optimization in place users will experience significant performance degradation, in-particular this will impact those links and sites with high latency.





| | Type ⬍ | Count ⬍ | Percent ⬍ |
|---|---|---|---|
| 1 | Error | 410575 | 56.17% |
| 2 | No Error | 320330 | 43.83% |



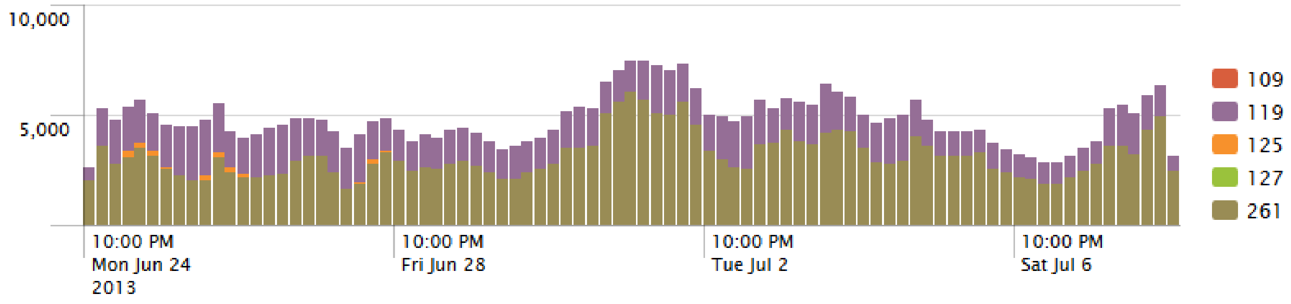
In this report, we see that more than 55% of the CIFS/SMB2 sessions were not being optimized as we would expect. It is normal that some sessions will not be optimized successfully, however this figure should be less than 1%, so 55% is extremely high and corrective action should be taken to address this.

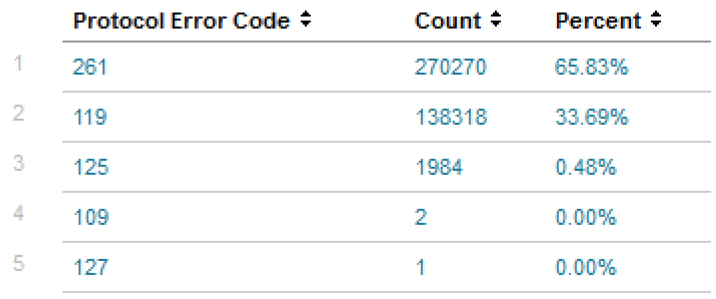
# Protocol Errors

When a protocol error occurs, the Steelhead lists a reason why the event occurred. . There will be many different causes, the most common are SMB-signing or SMB2 not enabled, but is can also be that the client or server operating system is not supported.

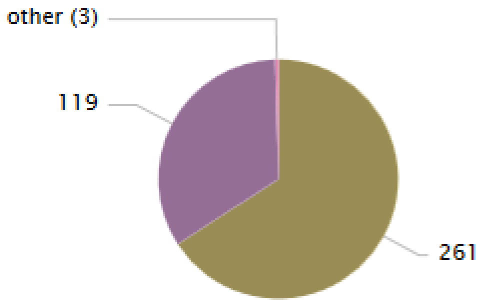
The protocol error code list is the 'official' Riverbed one and is available from the Riverbed knowledge base or from the appendix to this report.

This view is global, but in later sections you will be able to see what Steelheads, servers or clients are causing the errors.





| | Protocol Error Code | Count | Percent |
|---|---|---|---|
| 1 | 261 | 270270 | 65.83% |
| 2 | 119 | 138318 | 33.69% |
| 3 | 125 | 1984 | 0.48% |
| 4 | 109 | 2 | 0.00% |
| 5 | 127 | 1 | 0.00% |



In this environment we can see 5 different protocol errors, however only error 261 and 119 is of priority.

## *Error 261 - SMB2 blade disabled*

This error code is generated when the Steelheads SMB2 blade is not enabled. Older Steelheads do not have SMB2 optimization capabilities or enabled by default, and therefore traffic has no layer7 optimization. This error means users experience a significant performance penalty as they can only benefit from the "Data Streamlining" (data reduction) and not the "Application Streamlining" (Layer7). SMB2 is supported in RiOS 6.5 and later and Steelhead Mobile 4.0 and later.

**Recommendations**

As all Steelheads in this environment run versions of RiOS that support SMB2 optimization it is recommended that the configuration is changed to enable this feature.

## *Error 119 - Security signatures are required on the server*

SMB-signing is a "man-in-the-middle" countermeasure, preventing an attacker from manipulating traffic in transit. As the Steelhead is a man-in-the-middle device (although-the good kind), SMB signing prevents the Steelheads from delivering layer 7 optimization. However, since RiOS v5.5 SMB-signing has been supported, but more importantly support for Windows 7 and Windows 2008 servers was not available until RiOS v6.5 was released.

Riverbed is continuously upgrading and simplifying the SMB-signing support in the Steelhead. In RiOS v7.x and v8.x Steelheads can be joined as a Read-Only Domain Controller (RODC), this greatly simplifie~~s~~ the configuration and error rate associated with NTLM authentication against the client.

If end to end Kerberos support is required RiOS v7 and above has to be used in combination with the Kerberos delegation user. Please refer to the Riverbed tech paper "Optimization in a Secure Windows Environment" for further details.

**Recommendations**
All the Steelheads in this environment are running RiOS 7.0.5d, it is recommended to join all Steelheads as RODC and enable NTLM delegation in transparent mode. This will allow the Steelheads to optimize most clients and servers (Windows XP, Vista, 7, 2003, and 2008) without further configuration. If there is a requirement in the Active Directory for the client to authenticate through the Kerberos protocol, a Kerberos delegation user (with domain replication privileges) must be configured in the active directory and added to the Steelheads. Please refer to the "Optimization in a Secure Windows Environment" tech paper on guides.

You can also (if company security policy allows) downgrade the SMB-signing requirement on the server/client from "required" to "enabled" in Active Directory (GPO policy), this will also solve the problem without changing settings on the Steelhead appliances.

## *Error 125 - CIFS parser shutting down due to error*

An unknown error occurred to the optimization. The optimization engine reports the error code but is not aware of any further details about the issue. There is a chance that INFO level logs (if available) can reveal further details. However since the number of sessions that within an acceptable level, it is out of scope of this report.

**Recommendations**
There have been so few of these errors (less than 1%) and they are within the anticipated volumes in an installation of this size, no further action is required.

## *Error 109 - Negotiate response contains older CIFS dialect*

The server or the client is talking a CIFS dialect that is not supported (~~it's~~ considered obsolete). Upgrading the server or client is the only path to ~~have~~ enable ~~this~~ optimized ~~with~~ "Application Streamlining"

**Recommendations**
There have been so few of these errors (less than 1%) and they are within the anticipated volumes in an installation of this size, no further action is required.

## *Error 127 - UNKNOWN_SHUTDOWN_ERROR*

An unknown error occurred to the optimization. The optimization engine reports the error code but is not aware of any further details about the issue. There is a chance that INFO level logs (if available) can reveal further details. However since the number of sessions that within an acceptable level, it is out of scope of this report.

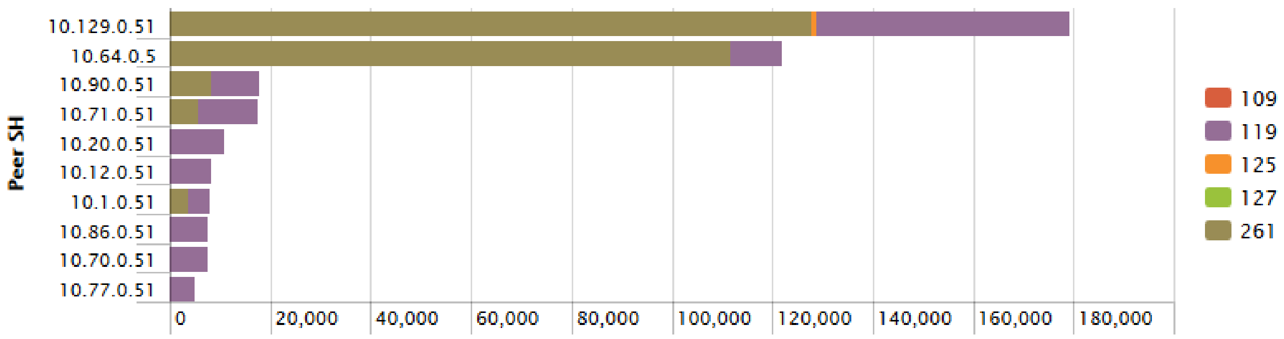
**Recommendations**

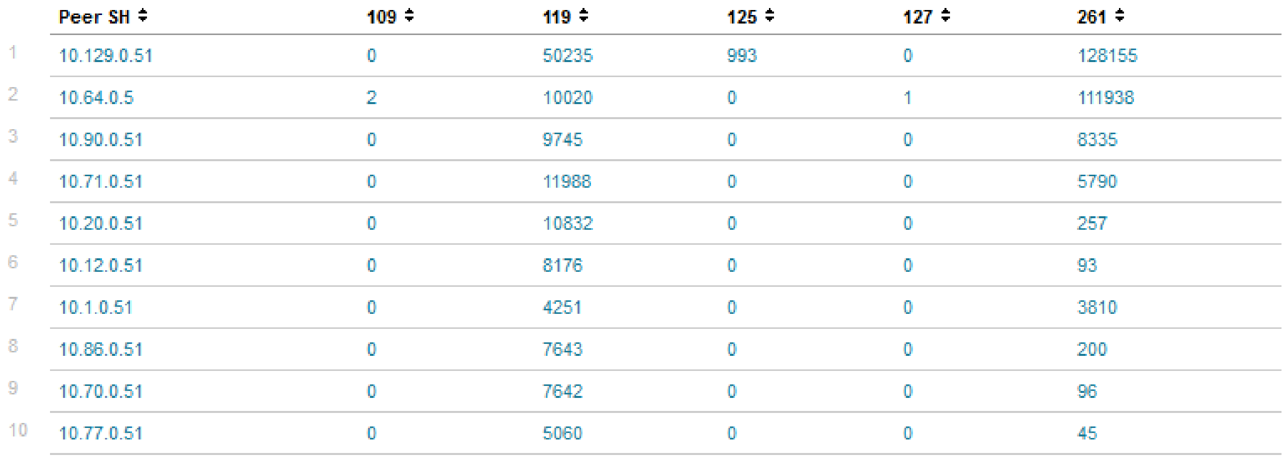
There have been so few of these errors (less than 1%) and they are within the anticipated volumes in an installation of this size, no further action is required.

# Top10 Steelhead Peers with Errors

When we analyze a session, data is collected to identify the server-side Steelheads. We use this information to detect Steelheads that have problems, helping you to identify and prioritize the Steelheads that need to be focused on when troubleshooting issues.

Note that the IP addresses are the In-path interfaces, this means that the same Steelhead can show up one or more times depending on how many interfaces it has.



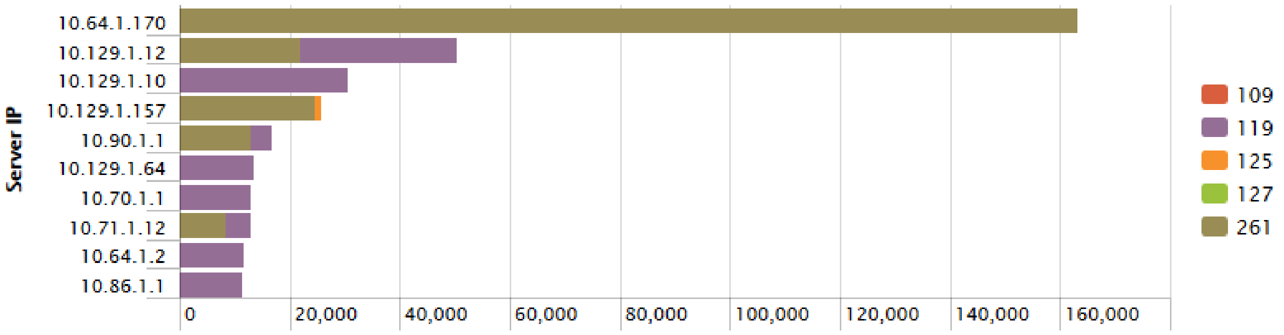


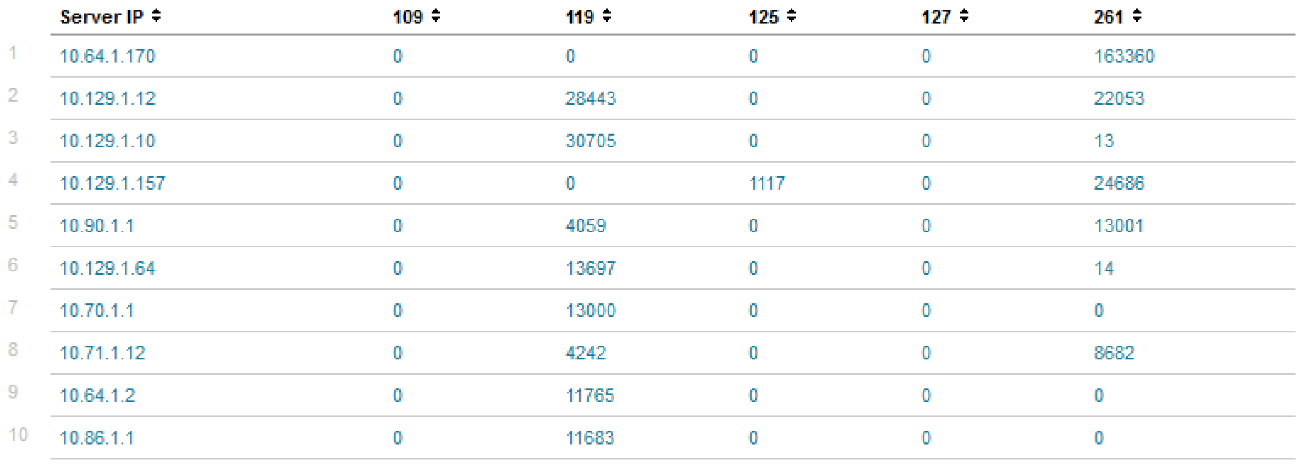
| | Peer SH | 109 | 119 | 125 | 127 | 261 |
|---|---|---|---|---|---|---|
| 1 | 10.129.0.51 | 0 | 50235 | 993 | 0 | 128155 |
| 2 | 10.64.0.5 | 2 | 10020 | 0 | 1 | 111938 |
| 3 | 10.90.0.51 | 0 | 9745 | 0 | 0 | 8335 |
| 4 | 10.71.0.51 | 0 | 11988 | 0 | 0 | 5790 |
| 5 | 10.20.0.51 | 0 | 10832 | 0 | 0 | 257 |
| 6 | 10.12.0.51 | 0 | 8176 | 0 | 0 | 93 |
| 7 | 10.1.0.51 | 0 | 4251 | 0 | 0 | 3810 |
| 8 | 10.86.0.51 | 0 | 7643 | 0 | 0 | 200 |
| 9 | 10.70.0.51 | 0 | 7642 | 0 | 0 | 96 |
| 10 | 10.77.0.51 | 0 | 5060 | 0 | 0 | 45 |

This table shows that two Steelheads account for the majority of errors – IP Addresses 10.129.0.51 & 10.64.0.5.  We recommend these two appliances are prioritized for investigation and corrective action.

# Top10 Servers with Errors

Within this section of the report we identify the servers causing the issues. It could be that a server is running a CIFS/SMB version or operating system that is not supported. Furthermore you can use this section to prioritize between servers/locations that have higher business priority.





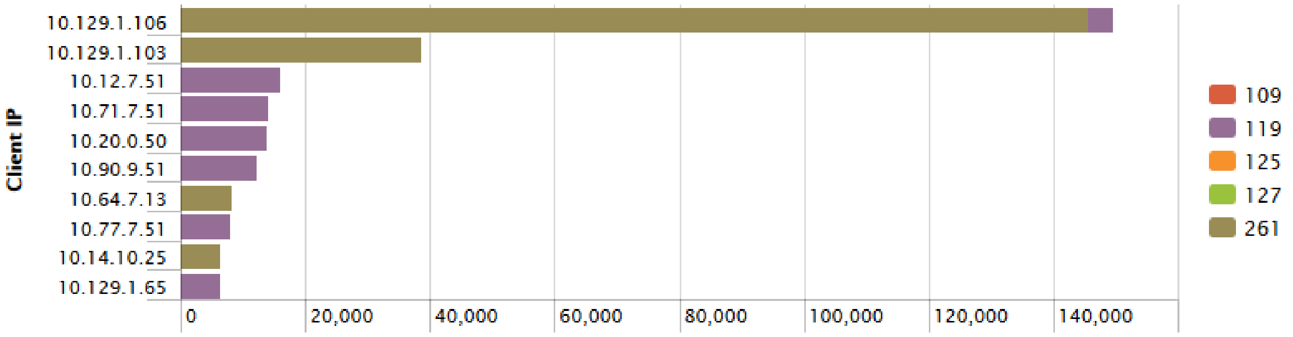
| | Server IP ⇕ | 109 ⇕ | 119 ⇕ | 125 ⇕ | 127 ⇕ | 261 ⇕ |
|---|---|---|---|---|---|---|
| 1 | 10.64.1.170 | 0 | 0 | 0 | 0 | 163360 |
| 2 | 10.129.1.12 | 0 | 28443 | 0 | 0 | 22053 |
| 3 | 10.129.1.10 | 0 | 30705 | 0 | 0 | 13 |
| 4 | 10.129.1.157 | 0 | 0 | 1117 | 0 | 24686 |
| 5 | 10.90.1.1 | 0 | 4059 | 0 | 0 | 13001 |
| 6 | 10.129.1.64 | 0 | 13697 | 0 | 0 | 14 |
| 7 | 10.70.1.1 | 0 | 13000 | 0 | 0 | 0 |
| 8 | 10.71.1.12 | 0 | 4242 | 0 | 0 | 8682 |
| 9 | 10.64.1.2 | 0 | 11765 | 0 | 0 | 0 |
| 10 | 10.86.1.1 | 0 | 11683 | 0 | 0 | 0 |

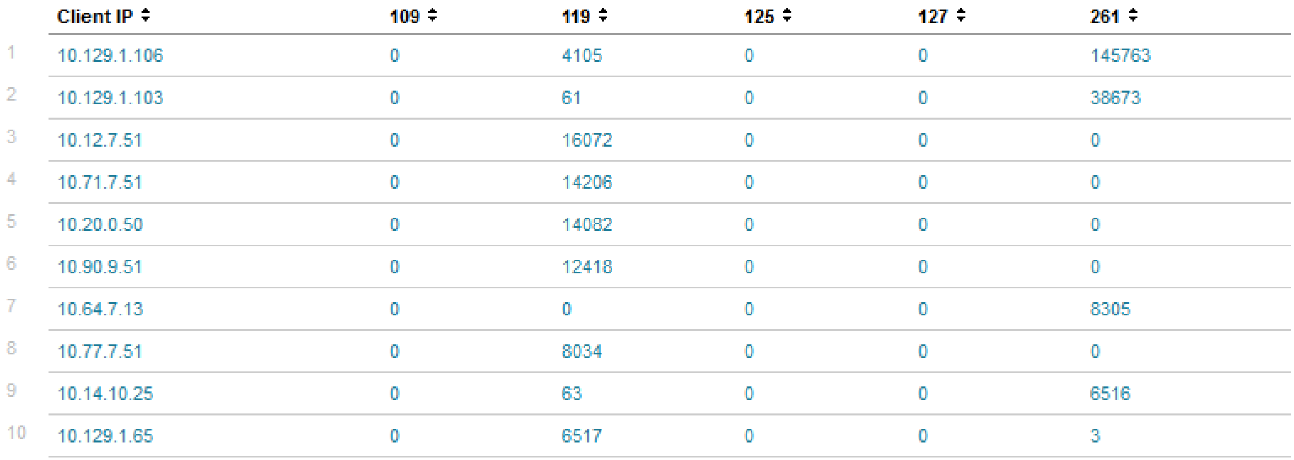
The table above identifies one server that generating a high number of issues - 10.64.1.170. This server is running SMB2, however it is very likely that the Steelhead at this location is not enabled for SMB2 optimization (error code 261).

The 2nd server on the list - 10.129.1.12 is likely to be a domain controller as it is also generates SMB signing (error code 119).

# Top10 Client with Errors

Within the section of the report we identify the clients that are causing issues. Like the server section it could be that the client is running a CIFS/SMB version or operating system that is not supported. You can also use this section to prioritize between clients/locations that have higher business priority.





| | Client IP ⇕ | 109 ⇕ | 119 ⇕ | 125 ⇕ | 127 ⇕ | 261 ⇕ |
|---|---|---|---|---|---|---|
| 1 | 10.129.1.106 | 0 | 4105 | 0 | 0 | 145763 |
| 2 | 10.129.1.103 | 0 | 61 | 0 | 0 | 38673 |
| 3 | 10.12.7.51 | 0 | 16072 | 0 | 0 | 0 |
| 4 | 10.71.7.51 | 0 | 14206 | 0 | 0 | 0 |
| 5 | 10.20.0.50 | 0 | 14082 | 0 | 0 | 0 |
| 6 | 10.90.9.51 | 0 | 12418 | 0 | 0 | 0 |
| 7 | 10.64.7.13 | 0 | 0 | 0 | 0 | 8305 |
| 8 | 10.77.7.51 | 0 | 8034 | 0 | 0 | 0 |
| 9 | 10.14.10.25 | 0 | 63 | 0 | 0 | 6516 |
| 10 | 10.129.1.65 | 0 | 6517 | 0 | 0 | 3 |

It's worth noticing that the Client 10.129.1.106 is by far the most active client (with errors), it is likely that is communicates with the server 10.64.1.170 seen in the previous section. This client is also experiencing common SMB2 issues.

# Apendix - Protocol Error Codes

| Protocol Error | Error Description |
|---|---|
| 102 | Client sent unhandled NT Transact request type |
| 103 | Client sent unhandled request type |
| 104 | Client sent unhandled Trans2 request type |
| 109 | Negotiate response contains older cifs dialect |
| 111 | UNKNOWN_SHUTDOWN_ERROR |
| 112 | Session setup request contains older cifs dialect |
| 113 | SMB_SHUTDOWN_ERR_BAD_SSETUP_REQ<br>See: https://supportkb.riverbed.com/support/index?page=content&id=S15714 |
| 116 | Tree connect response contains older cifs dialect |
| 118 | Security signatures are enabled on the server |
| 119 | Security signatures are required on the server |
| 122 | Server returned duplicate FID |
| 123 | UNKNOWN_SHUTDOWN_ERROR |
| 124 | Unable to optimize SMB2 traffic |
| 125 | Cifs parser shutting down due to error - Disabling latency optimization - only bandwidth will be optimized |
| 126 | Cifs parser shutting down due to error - Disabling latency optimization - only bandwidth will be optimized |
| 127 | UNKNOWN_SHUTDOWN_ERROR |
| 128 | UNKNOWN_SHUTDOWN_ERROR |
| 258 | UNEXPECTED_SMB2_TRAFFIC |
| 259 | SIGNING_IN_USE (SMB2 signing required) |
| 261 | SMB2 blade disabled |
| 262 | SMB2 Connection Blacklisted |
| 263 | UNSUPPORTED_DIALECT |