***Network Analysis Example Document Version 1.0***
***by Brandon Hitzel (www.networkdefenseblog.com)***

This is a network assessment document I have created in order to help people with showcasing troubleshooting data in a presentable format to possibly prove innocence or help locate the problem. The idea is to look at every aspect of the network, or the network devices at a specific remote site in order to determine if there are any issues or to prove there are no issues. After that the next group can take over the troubleshooting like desktop, server, application etc.

This isn't something you'd generally create with 1 ticket, this is something you'd create after receiving 20 of the same tickets/complaints over time (chronic issue). Although the 1 ticket rule has an exception for something like a deep analysis to prove poor application performance isn't network related.

Ideally you will create this in microsoft word but if you don't have that google docs or other free documents editors I'm sure will work. Its preferable to have tools in order to take screenshots, this helps graphically supplement the analysis write up.

Remember you are trying to eliminate the network so you need to write things like , "no issue found", "generally if there was a problem x would be seen" or "this would point to a problem" if you found something wrong within your domain etc. Additionally it's good to provide background/baseline info before beginning. The conclusion is key to provide recommendations or to list what problems you found and the steps you will take to resolve them.

- Items in **bold** and *italicized* are ***notes/descriptions***.
- Items *italicized* and with <> are generalized examples
- Regular text will be periodically shown with **Example:** to show it is example text.

*Be sure to use Text Wrap (inline) to move pictures around and not have to worry about where the text cursor is. Also I use windows snippet to pull images from my tools or reports. After completion export to PDF, verify formatting, and send :).

*****Feel free to use this format at your discretion but do not copy this doc and claim it as your own. All items contained within this document are fictional examples and should not actually be used outside of this document. *****

***Begin of the example document this is page 1***

# <Network Analysis Template>
# December 2018
# By <team or company>

## Contents





***Insert company, application, and/or customer logos here***

# Part 1 – Introduction

***This is where you will list the background of the network or the specifics for the remote site. It's a place to list the reason for doing the assessment, like the customer is complaining of slowness or there has been multiple recent outages for the site, a specific application has chronic poor performance, or the customer has a large business event which is dependent on the network etc. Use it to lay the groundwork and provide some context.***

**Example:** The *<location>* is a campus which has one WAN circuit that provides external connectivity back to HQ for multiple locations including *<building location #1>* and *<key location #2>*. The site has seen heavy usage over the years and with the recent campus construction, multiple groups have been moving around consistently to different buildings. *< your IT Group name>* has seen the usage and has performed multiple bandwidth upgrades on the site. On *<date/year>* the upload bandwidth was increased from 50mb to 100mb. Furthermore, the core switch was upgraded to a better model recently in *<date/year>* after follow up meetings with *<local POC or supervisor etc.>*. Once the 100mb upgrade was completed there was a significant drop in latency as observed by our tools.

In addition to upgrading the available bandwidth, circuit throughput tests have been performed on <*date/time*> simulating <*TCP/SMB/protoco*l> traffic. There were no issues found in our throughput tools.

The hardware, configuration, and overall setup up of the site conforms to other sites as a part of *<company/group>* network standards *(hopefully you have standards)*. Moreover, traffic is routing correctly as designed to the core network device at *<Aggregation point >* and has been stable for multiple weeks. Although the network is very simple and only forwards traffic from A to B, it has the highest possible end-to-end visibility. Using this capability provides an accurate look into what is going on behind the scenes of the daily device interactions.

# Part 2 – Analysis Criteria

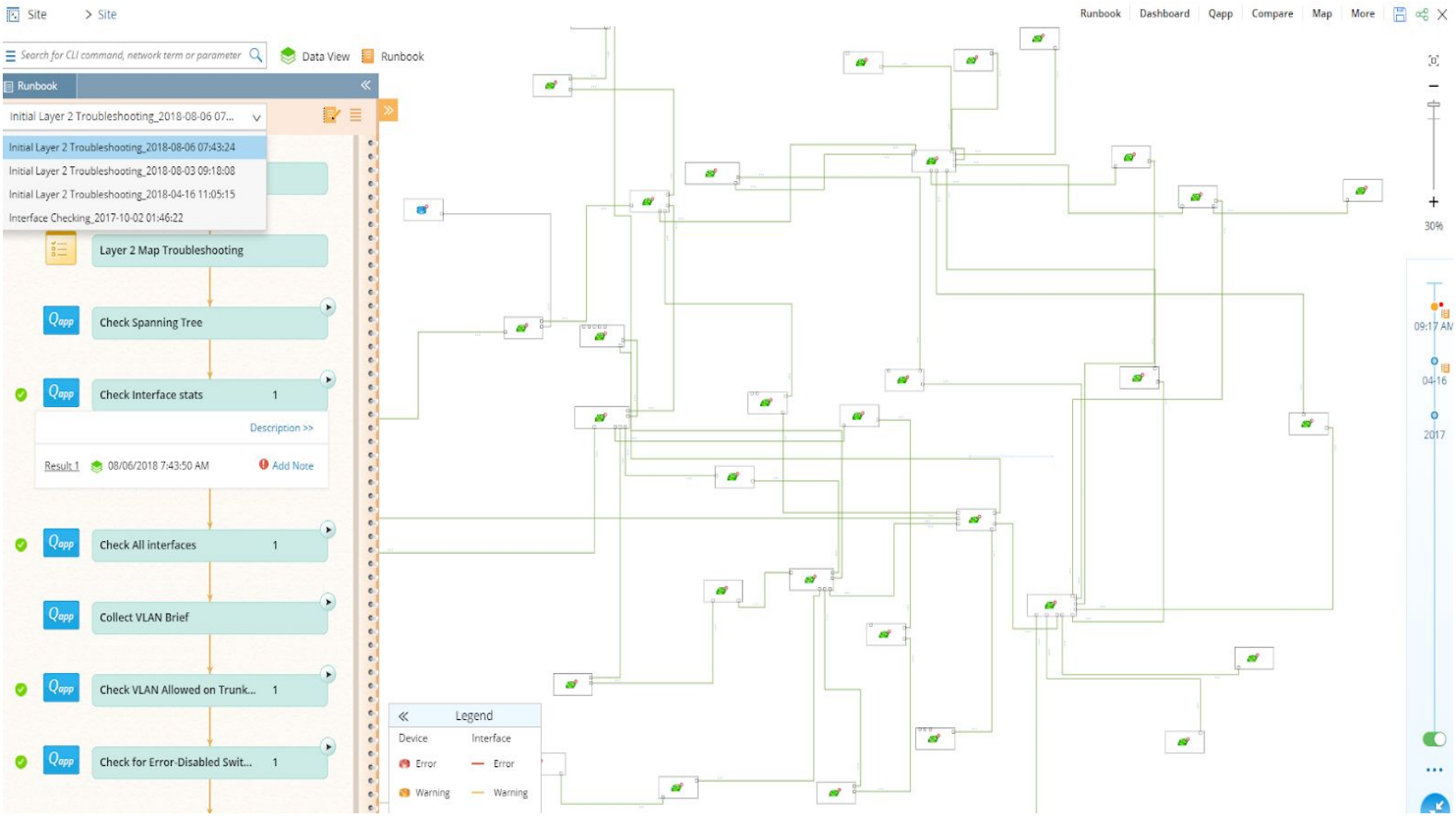
***This where you can list some of your tools or methods you use for the analysis, see the below example***

a) **Example:** *<IT Group name>* uses a variety of tools to troubleshoot and analyze issues like this. Some tools also preemptively identify issues to help the team proactively address items before they become a larger problem.
b) Performance tools capture multiple types of information like bandwidth utilization and application data to store for future historical comparisons.
c) In-depth knowledge and experience of networks is something that is used by our team to provide accurate analysis of data whether historical or live.
d) A comprehensive approach encompasses the review of bandwidth reports, application data (including source & destination address and port), network round-trip-time (RTT), hardware CPU/memory utilization, on-site testing, packet capturing review, configuration standards verification, and firewall IPS check.

# Part 3 – Graphical Tool/Topology/Interface errors etc.

***Here you display the graphical topology, with a tools like Netbrain, Intermapper, auvik etc. You could also just show a network diagram, maybe a logical and physical showcase of the location w/ visio if you don't have a graphical tool. Mention if you did any troubleshooting or verification of items. Here we talk about running scripts to check for errors and duplex mismatches on interfaces and verifying the switch configurations, obviously this could also be done manually if automation isn't used.***

a) **Example:** NetBrain is a tool that is able to provide a graphical representation of the network to troubleshoot in real time.
b) NetBrain scripts have been ran a few times for <*location in question*> in order to determine if there are any physical or configuration issues. It was able to verify that the configuration on all of the switches conformed to the <*company*> network standard.




c) NetBrain was also used to check every interface from end-user to uplink connection for errors. 1 access port was identified to have errors but the problem appears to have subsided. This would not have affected other user's network experience. If any lines above were red, that would indicate a problem with duplex or errors(it's a scripted item within the troubleshooting tool).

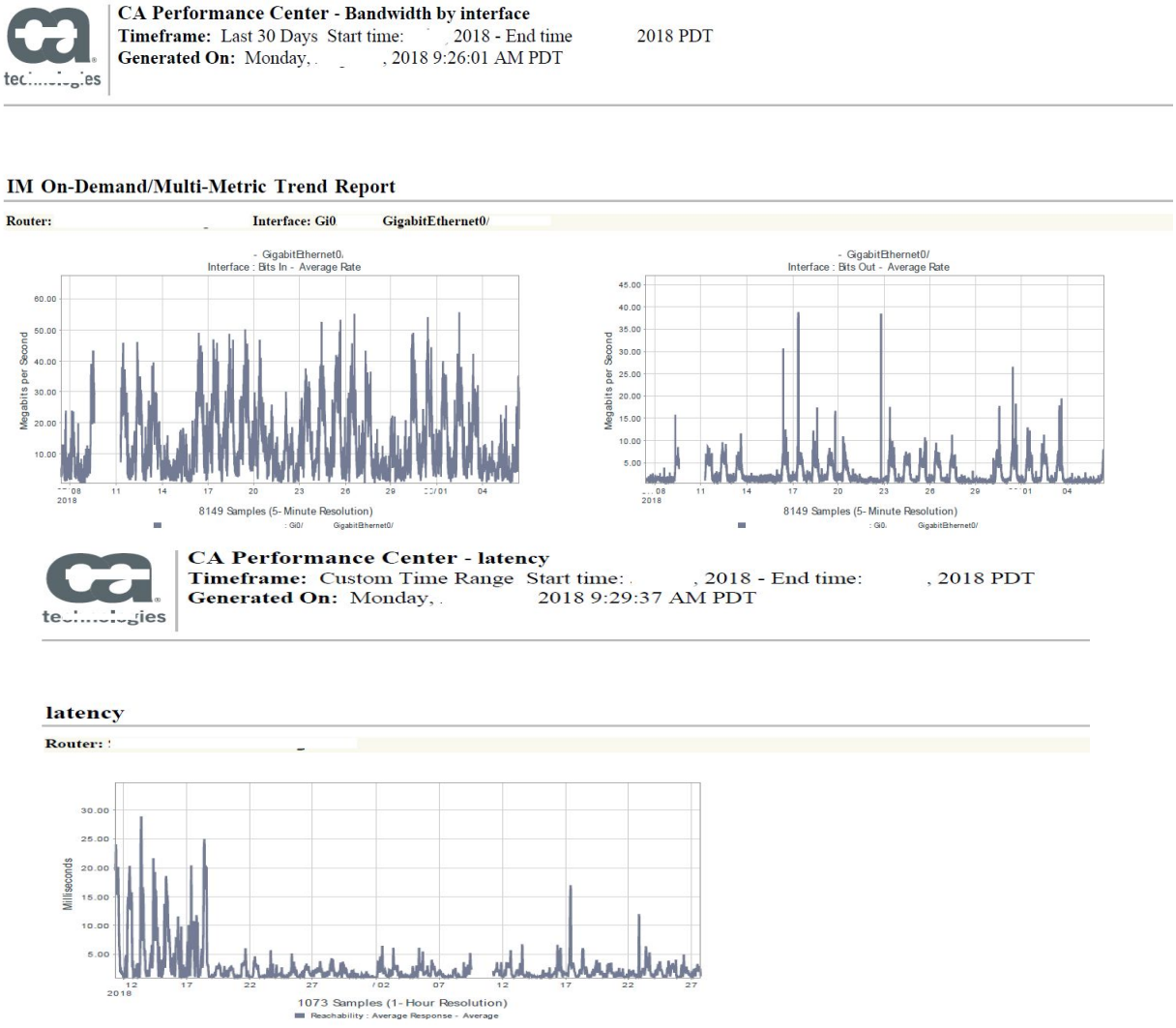
# Part 4 – Performance Tool – Bandwidth and Hardware Reports

***This is where you review bandwidth reports, CPU, memory utilization w/ CA, solarwinds, PRTG etc. Remember to review 95th percentile for bandwidth reports if possible.***

a) **Example:** <*Performance tool*> is used to poll interfaces for traffic in & out along with errors. Devices are polled for their CPU and memory utilization to be stored historically. Excessive utilization in any of these areas could cause network slowness. It should be noted that the site's available trusted non-guest bandwidth is <*Mb*> for uploads and downloads; this would be considered <*high/low*> compared to other locations.

b) The top report from the last 30 days show utilization under maximum, with a few spikes. This is for the trusted non-guest bandwidth only, upload and download. Max is <*Mb*> download (in), <*Mb*> upload (out). Moreover, there were over 200 samples taken per day over this period.

c) The second graph shows the latency before and after the recent <*change/upgrade*> on <*date*> notice the sharp drop in latency (performing better/faster) after the upgrade.



# Part 4 – Performance Tool – Bandwidth and Hardware Reports

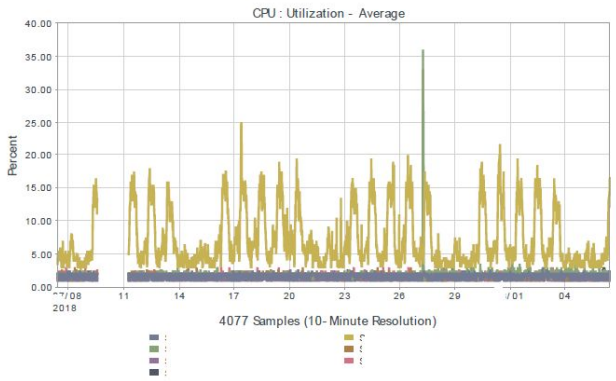
d) **Example:** The next graph is the CPU and memory utilization of the core devices for each of the *<campus>* locations. The average CPU usage is under 25% and memory under 50% which is good.

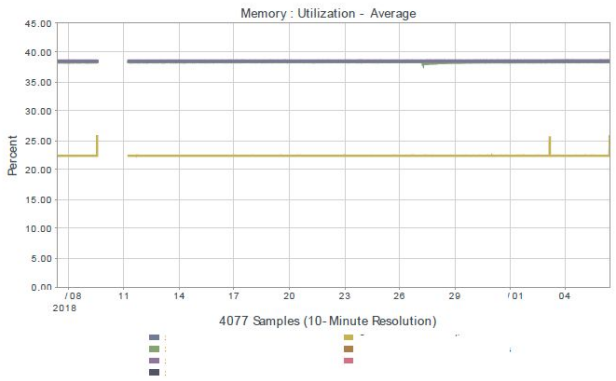
e) This last graph shows the average response time for the main distribution switches at the site's *<building #1>* and *<key location #2>*. Although some spikes were observed, the average is consistently low (good).

**CA Performance Center - router health**
**Timeframe:** Last 30 Days Start time: , 2018 - End time: , 2018 PDT
**Generated On:** Monday, , 2018 9:52:27 AM PDT

**IM On-Demand/Multi-Metric Trend Report**

**(multiple items)**

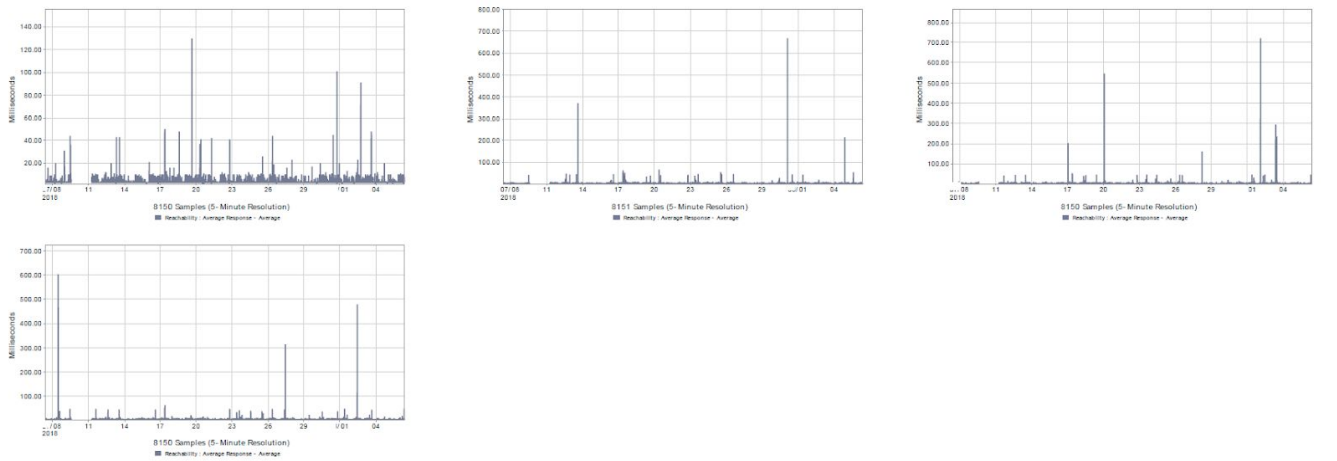



**CA Performance Center - latency**
**Timeframe:** Last 30 Days Start time: , 2018 - End time: , 2018 PDT
**Generated On:** Monday, 2018 9:40:21 AM PDT

**latency**

**(multiple items)**

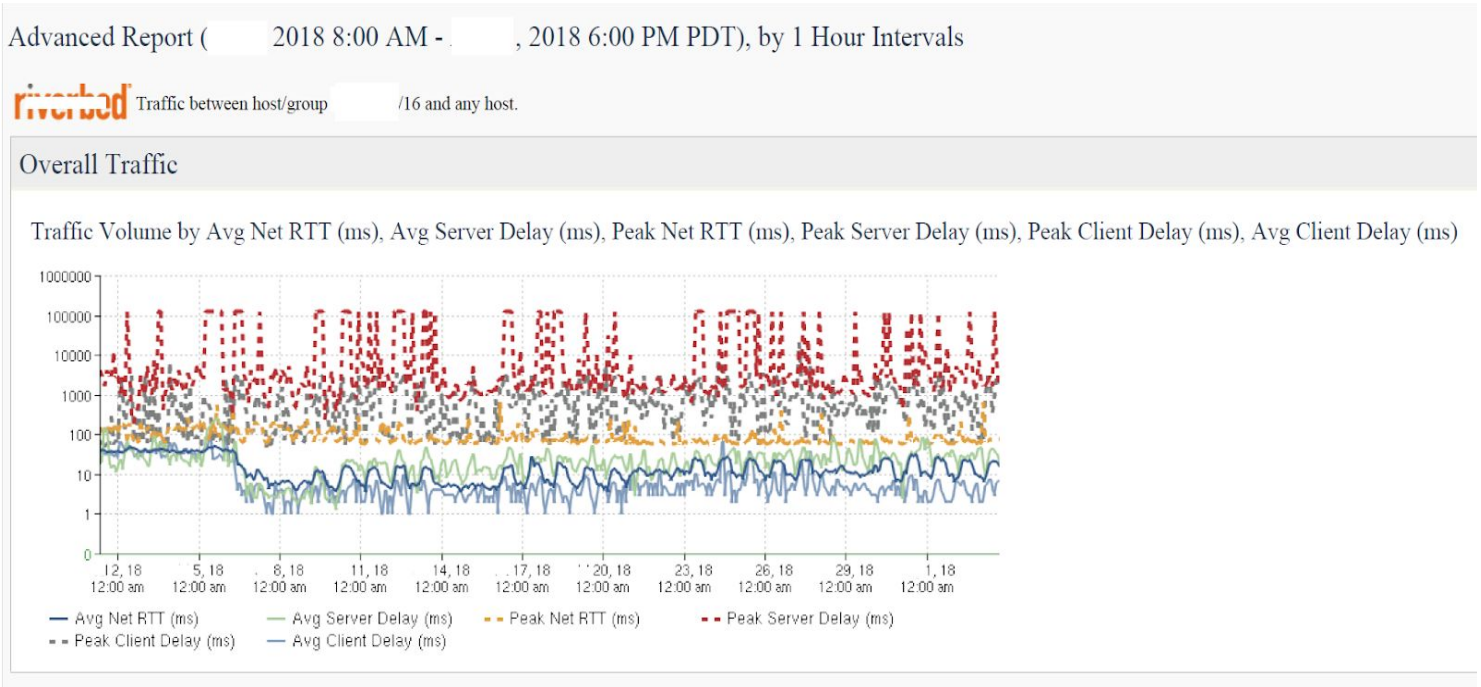


# Part 5 – Flow Tools – Netflow Reports

***This is where you put your net flow, jflow or sflow etc. reports. these are great reports if you can get them. Also if this report is for an application specific issue, these reports are key to possibly show where the slowness is.***

a) **Example:** Riverbed Cascade is a useful tool that aggregates all of the traffic in the *<company>* network. The tool shows conversations between devices (i.e. Source and destination); plus it shows the application ports used and how much traffic was transferred during that conversation. Furthermore, it is able to measure the network round-trip-time (RTT), server delay, TCP protocol retries (i.e. Traffic had to be retransmitted), along with other data parameters.

b) Data was aggregated from the *<location's>* IP address subnets to measure overall network RTT for the last 30 days. On average the network delay was very low (~10ms) which is fast. Server delay was generally higher but this could be caused by many factors including the type of file being transferred and application being used. In addition it should be noted that that the peak client and server delay were higher on average than the peak network delay.




c) **Example:** The top application for the site (during the report period) appears to be TCP port 445 (Microsoft-ds) to/from storage servers which could be file transfers among other things. File transfers generally have a high tolerance for any network latency variations or errors, however the type of file and protocol along with the end system drastically affects the user experience. Things like excessive interface bandwidth or server hard drive utilization could also cause slowness.

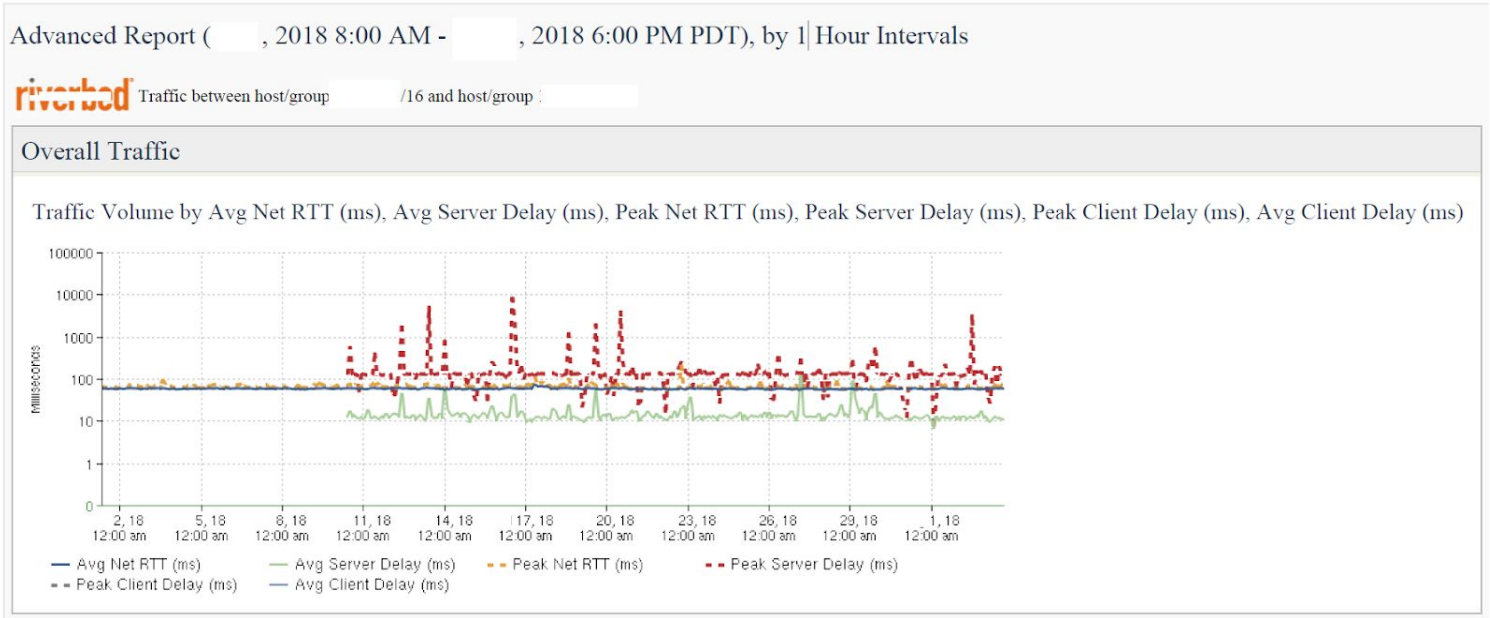
# Part 5 – Flow Tool – Netflow Reports continued

d) **Example:** This shows the top 12 users by utilization for the site for the last 30 days. Notice *<app name>* for many users.

Host Pair with Port 1 - 200 of 10000

| Server | Server Group | Client | Client Group | Port | Avg Bits/s | Avg Packets/s | Avg Active Connections/s | Avg Net RTT (ms) | Avg Server Delay (ms) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | tcp/445 (microsoft-ds) | 342,481 (2%) | 39.35 (1%) | < 0.01 (< 0.01%) | 34 | 4 |
| | | | | | 260,415 (1%) | 36.06 (1%) | < 1 (< 1%) | 58 | 15 |
| | | | | | 247,443 (1%) | 34.26 (< 1%) | < 1 (< 1%) | 58 | 14 |
| | | | | tcp/445 (microsoft-ds) | 196,002 (1%) | 25.07 (< 1%) | < 0.01 (< 0.01%) | 47 | 2 |
| | | | | tcp/80 (http) | 151,228 (< 1%) | 21.03 (< 1%) | < 1 (< 1%) | 59 | 16 |
| | | | | tcp/80 (http) | 143,583 (< 1%) | 19.95 (< 1%) | < 1 (< 1%) | 60 | 12 |
| | | | | tcp/80 (http) | 117,919 (< 1%) | 16.42 (< 1%) | < 1 (< 1%) | 57 | 14 |
| | | | | | 102,734 (< 1%) | 14.13 (< 1%) | < 0.01 (< 1%) | 38 | 4 |
| | | | | tcp/80 (http) | 98,537 (< 1%) | 13.72 (< 1%) | < 1 (< 1%) | 61 | 16 |
| | | | | tcp/80 (http) | 89,374 (< 1%) | 12.60 (< 1%) | < 1 (< 1%) | 60 | 17 |
| | | | | | 88,516 (< 1%) | 12.45 (< 1%) | < 1 (< 1%) | 57 | 13 |
| | | | | tcp/80 (http) | 88,129 (< 1%) | 12.23 (< 1%) | < 1 (< 1%) | 58 | 11 |
| | | | | tcp/445 (microsoft-ds) | 87,330 (< 1%) | 9.91 (< 1%) | < 0.01 (< 1%) | 35 | 1,063 |

e) The top unique application appears to be *<app name>*, which is a SaaS hosted app. The below report was run between the site users' PC and this specific application server only. Network round trip time looks consistently around the 40-50ms area due to the fact it is going to the *<cloud/on prem>* data center. Server response times also look consistently low, however there were latency spikes observed from the server side. That could be where the slowness is located (server side).



# Part 6 – Wireless

***Wireless doesn't always play into the equation for application specific slowness, but if you are assessing an entire location then it's good to include. Check for over utilized access points. Also things like cisco clean air or ruckus smartcell insight reports would be useful.***

a) **Example:** Some traffic from users travels through *<company>* wireless network. The wireless access points are all configured the same as all other *<company>* venues. Moreover, the hardware models are all the same and they use the same controller cluster. Internal non-guest bandwidth is shared at these campus locations between wired and wireless. There could be issues with coverage in *<building>* because it does not have enough Wireless Access Points for full coverage. Location surveys and recommendations have been provided in the past.
b) The maximum connected clients to a WAP doesn't appear to exceed 25 (in the reporting period). Having 25 or more clients on 1 access point at the same time could cause performance issues for those clients on that particular access point.
c) The top utilized wireless access point is *<WAP name>* at *<location x>*. There could be a project to add a couple additional WAPs in the near future to the <affected area> which should help with wireless coverage and performance if *<user department>* requests it.

**Most Utilized by Maximum Concurrent Clients**

| RANK ▲ | AP/DEVICE | MAX CLIENTS | UNIQUE CLIENTS | TOTAL DATA | AVG USAGE | LOCATION | CONTROLLER | FOLDER |
|---|---|---|---|---|---|---|---|---|
| 1 | WAP0 | 21 | 75 | 55.06 GB | 154.49 Kbps | Outside | | |
| 2 | WAP | 21 | 44 | 21.25 GB | 59.63 Kbps | Outside | | |
| 3 | | 14 | 31 | 3.53 GB | 9.90 Kbps | 1ST_FL | | |
| 4 | | 13 | 71 | 46.64 GB | 130.87 Kbps | | | |
| 5 | | 9 | 24 | 430.20 MB | 1.21 Kbps | | | |
| 6 | | 9 | 22 | 1.81 GB | 5.08 Kbps | | | |
| 7 | | 8 | 16 | 1.48 GB | 4.14 Kbps | | | |
| 8 | | 7 | 6 | 4.97 MB | 0.01 Kbps | | | |
| 9 | | 5 | 21 | 1.12 GB | 3.14 Kbps | | | |
| 10 | WAP0 | 5 | 8 | 0 MB | 0 Kbps | 2ND_FL | | |

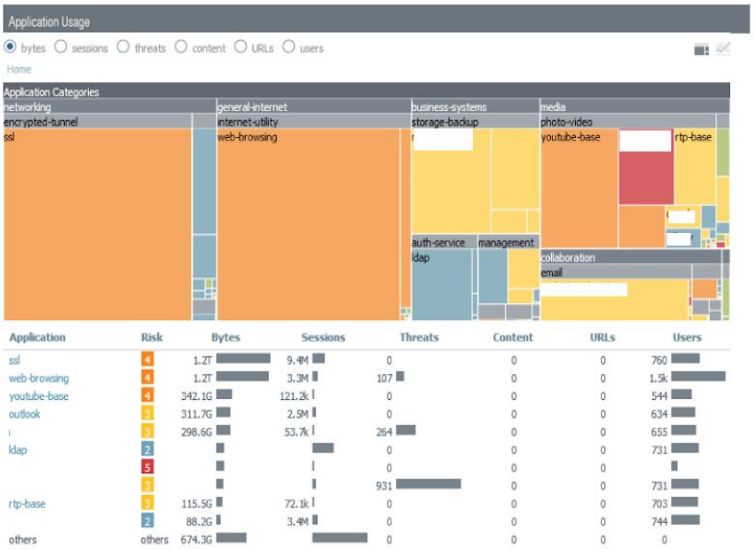
# Part 7 – Firewall/IDS/IPS or Pcap analysis

***Firewalls are blamed a lot for issues, so be sure to include some useful graphs if possible. Also if you have an IPS inline to the location be sure to check that for blocks/drops. In addition, if you have the ability to capture packets, a pcap assessment would be good to list in here.***

a) **Example:** Traffic from this site and many others travels through our <*vendor's*> Firewall. We are able to view traffic paths, file transfers, and also capture packets. We can see what is happening at a detailed level for traffic flows. Lastly, the firewall is designed to drop or block suspicious traffic including malware, we can see if there are excessive drops or blocks that could impact the user experience.

b) Sometimes traffic is classified as malicious when it is not and is dropped, this is called a false positive. We did see some <*application #1*> and <*application #1*> traffic in the threat analysis but it was not getting blocked; therefore the false positives are not negatively affecting user experience (these are simply application classification levels). The important thing is the heavily used <*previously mentioned app name*> application is not being classified as a threat. The report was taken from our <*core/distro/DC etc.*> firewall and shows locations <*previously mentioned locations*>.

c) There were two packet capture sessions performed on two test PCs. The packet capture is essentially looking at the traffic with a microscope, there is no deeper way to look other than this. The delta (response) times between traffic sent and traffic received were within acceptable levels. However there were delays seen from the server side, consequently users would be seeing slowness due the time having to wait for information to be delivered from the server.




# Part 8 – On-site testing/throughput tests etc.

***Here you can put any on-prem testing you did using tools like iperf or Wireshark etc. Sometimes the network or security teams will need to put on their server or desktop hats. It could require you to bring a laptop on site to test yourself or perhaps you performed some throughput tests during peak and after hours to compare performance.***

a)**Example:** The network team went to the <*location*> on <*date/time*> to test file transfer throughput from the user's PC in question to the primary application server. Using our TCP tool we were seeing <*throughput totals*> which would be considered very high. However during peak times of performing the same test performance was significantly less (<*throughput total*>), there were no bandwidth issues during this time so it is recommended to review storage and server health during this time. A publically available speed test to the internet was also performed during peak times which had acceptable results.

b) The below table showcases the results from the <*teams*> testing.

| Test Type | Date/Time | Location | Upload BW | Download BW |
|---|---|---|---|---|
| Speedtest.net | 12/14 - 11am | User Joe PC on-prem | 250Mb/s | 300Mb/s |
| TCP throughput | 12/14 - 11am | User Joe to server 1 | 95Mb/s | 560Mb/s |
| TCP throughput | 12/14 - 11pm | User joe to server 1 | 450Mb/s | 890Mb/s |

# Part 9 – Conclusion and Recommendations

***The conclusion is where everything is brought together. You need to list the steps you took and your findings. Did you find a problem that needs correction? or Did you not find a problem but have a recommendation? Also if you did on-site testing this would be a good time to mention it again.***

a) **Example:** In conclusion, based on the data analyzed, the troubleshooting tasks performed, and the captured data we can conclude that there are no network related issues present at *<location>*. The user experience is likely being negatively affected by a defect within the application, the client/server process for the particular application, the server hardware, or the operating system/desktop.
b) The CPU, Memory, and bandwidth utilization for the network devices were all within acceptable levels.
c) The firewall was not blocking traffic intermittently which would have caused a performance problems. Also the session and CPU utilization is under utilized which is excellent.
d) Network round trip time is consistent and doesn't appear to have large slowness spikes. Although there was some elevated latency observed at the local site before the *<previously mentioned date> <upgrade/change>*, any slowness experienced after that wouldn't have been a side effect from the elevated latency.
e) It appears the top application being used is *<previously mentioned app>*. The average latency seen here for this app is around 40-50ms because it has to go to the *<cloud/on prem>* data center, so the application could react negatively because it cannot tolerate latency that high.
    a. Furthermore it appears it is using *<app port tftp,http etc.>*, so there could possibly be security and performance improvements to help the user experience by using SCP or SFTP.
    b. Also it would be good to make sure that this traffic is being optimized by the *<WAN optimizers/SD-WAN/tunnel etc.>* (if it can be) before it goes to the cloud.
f) **Example recommendation:** Due to the fact there doesn't appear to be any hardware or physical circuit issues with the site, a review of the user's desktops is recommended. Things to look at would be OS patching level, hard drive, NIC and hardware drivers, anything related to web browser, Group policy (GPO), AV software etc. Tests should be performed with new laptops and clean laptops not on the domain etc. to try and determine where the issue is.
**g)** **Example problems found:** After performing the in-depth analysis it was found that the Quality of service (QoS) policy was not configured properly on <device> and the issue was corrected. Moreover, it was found that some of the wireless access points were not deployed correctly, the IT team will continue to investigate the issue and follow up with a resolution shortly. etc etc.

***Hope this helps you, please like, share, and follow !***

***https://www.networkdefenseblog.com/blog***

**https://www.twitter.com/brandonhitzel**