Gmail

John Loop <pccitizen@gmail.com>

John Loop's 5-10-2021 imonitor[g] newsletter; cloud computing, microSD cards, raspberry pi0w, plot explanations
1 message

John Loop <jdloop@imonitorg.com>
To: "pccitizen@gmail.com" <pccitizen@gmail.com>

Wed, May 12, 2021 at 9:23 AM

Dear imonitor[g] users, potential users, former users, and interested parties:

Summary for those of you new to this newsletter:

> ***I [John Loop] am working on a project to perform Internet [and local network] performance monitoring. I use a small device [raspberry pi], along with custom scripts to perform this service. I have deployed this device to 23 "guinea pigs" across the country who help in the development. I initially targeted the service in 2018 to users in my mountain community in Jasper GA [windstream ISP] to assist in troubleshooting, but it is applicable universally, and I have "guinea pigs" across the country on Windstream, ATT, Spectrum, Comcast, CenturyLink, Tmobile and several other ISPs. It spans all access technologies from ADSL, VDSL, WADSL, cellular, cable and fiber. I also released a "generic" version which is completely standalone.***

Let me know if you are interested. OR you can purchase a raspberry pi 3B or 3B+, burn a microSD image [You can get it from sourceforge or I can send you one], and insert the pi in your network! ***Nerds might be interested in this alternative.*** You will get LOTs of info about your network!! Here is a 3B+ pi you can order: -just get a microSD image from sourceforge or from me, and you are in business.

https://www.amazon.com/gp/product/B07BLRSKBV/ref=ppx_yo_dt_b_asin_title_o00_s00?ie=UTF8&psc=1

As usual, to my "guinea pigs" ***I am extremely grateful for the use of your ISP connection and your help to develop this service across many ISPs.*** It has been invaluable, much fun, and the excuse for much discourse amongst old friends.

As always, you can refer to the main information page at https://imonitorg.com There are images of the web site, email, plots, etc.

There is a "quick intro" doc at https://imonitorg.com/QuickManual.pdf [also attached to this email] [there is a QuickManualG.pdf for the generic version as well]

Last month Newsletter: https://imonitorg.com/newsletter2-1-2021.pdf

Newsletter 6-1-2021 topics

1. Transition to new Linode cloud management server at imonitorg.com complete.

The managed raspberry pis [rpis] pi1-30 used by my "guinea pigs" are now reporting to a [linux of course] cloud server I created at linode.com. I have turned up a web server, mail, and ssh server to perform imonitor[g] duties. You will notice emails now come from jdloop@imonitorg.com. It has been an interesting experience. For $7 a month [including weekly image backups], it probably costs less than running a server here at home. I still have backup access using my server here, johnloop.com. Let me know if you want any additional details/experience. The only downside I have seen so far is the Linode [as is most any cloud svc] is used by Internet lowlife, and you may see my IP role on and off email blacklists. Not sure what to do about that.....

You can see the main web page and the performance plots from all the "guinea pigs" here:

https://imonitorg.com main web page.... go here for the plots [link middle of page]:

https://imonitorg.com/customerplots/customerplots.html [click on the top link for the plots, second link for customer list]

2. I have started work on a raspberry pi0w [pi0 wifi] implementation of imonitor[g].

Raspberry pi0w is wifi only, unlike the pi3Bs [which have ethernet], so I have had to install wifi AP [access point] software to allow the user to initially configure the wifi home parameters much like you configure your amazon, apple, etc wifi only devices [just login to the SSID broadcast and open a web browser to the pi0w to enter wifi parameters]. The pi0w costs almost nothing, and you can just plug it into the usb on your router with a short cable to power it, and it will perform all the performance monitoring tasks that the previous pi3Bs do. Info on the raspberry pi0w: https://www.raspberrypi.org/products/raspberry-pi-zero-w/

3. I have continued to update rpi 3B, 3B+ generic images [imonitorg] at sourceforge for completely standalone implementations [pi0 will be coming]

The latest update is 5-10-2021. These images run completely self contained, NO connection to third party servers, independent of my management, and will come up running once plugged into an ethernet port on your network -no configuration is necessary. You have only to find it on your network [ask your router], browse to it for all the network info. You can also configure a daily email using your gmail account as a relay [you will have to enable 2FA on your gmail account -which is a good idea in any case!]. https://sourceforge.net/projects/imonitorg/ All managed rpis [pi1-30] have daily email reports.

Going forward, I have not decided to created a pi4B image as of yet. pi0w seems more useful as a dedicated perf monitor machine.

4. Concerns about microSD storage

Over the past few years we have encountered problems with the microSD USB storage used by the rpi. These are the small memory squares, about 1/2" in size you use for most every gadget these days. I have made modifications to the software to lessen the write frequency to the microSD to lengthen its life. I am also selecting only "High endurance [or the like such as Sandisk High Endurance]" microSD cards going forward. The main intent of the microSD USB storage was STORAGE, for photos, videos, etc, and NOT for repeated use as an OS. This has become clear as we see a few of the pis die. The symptom can be very obscure, or obvious, as in mounting the FS "Read only." As of this date, pi9 [mark in GA] is currently offline due to a "read only" FS.

If you are gungho into this adventure, you can extract the microSD from the pi and copy and restore the image to a new microSD card [or just save a backup image-tho it may not contain updates after your image creation]. Many tools are available such as the "Win32 Disk Imager" which runs on windows 10. Other programs are readily available. Otherwise let me know and I can do this for your if you send me the microSD.

5. Work continues on bug fixing, stabilizing main code on pi3B, 3B+

In retrospect, the use of bash as the main coding is probably a mistake for a project which has grown to these dimensions [several thousand lines of bash code across dozens of scripts]. On the other hand, using bash is sort of like using single board computers to do your work instead of designing and building your own. Everything at the linux cmd line [which is second nature to many] is basically callable using bash without having to learn a new language syntax. And processors are fast enough to make up for any inefficiency in the coding -which are certainly many.

6. Additional network info collected [refer to the attached "manual" also]

Besides the performance monitoring of your Internet ISP [the original and main intent of this project], the rpi is also doing additional collection of network data. None of this data leaves your network, other than to be relayed to you via email via my server [and only for the pi1-30's]. It is available 24/7/365 via browsing to your local pi, who IP address is shown in the daily email. Some of this data is listed and described here:

a. Alerts [IP address changes, network hiccups, reboots -local pwr outage?] -sent via email

b. Speedtests and delay plots [archived plots for historical tracking and reference]

c. Wifi SSID networks and characteristics in range [very important if you live in a wifi maize!]

d. Hosts on network, and changes day over day -listing by IP address

e. Historical arp table showing you everybody who was ever on your network!!

f. [if enabled] service scan off your network, and changes day over day [very important if your network -wifi- is visible]

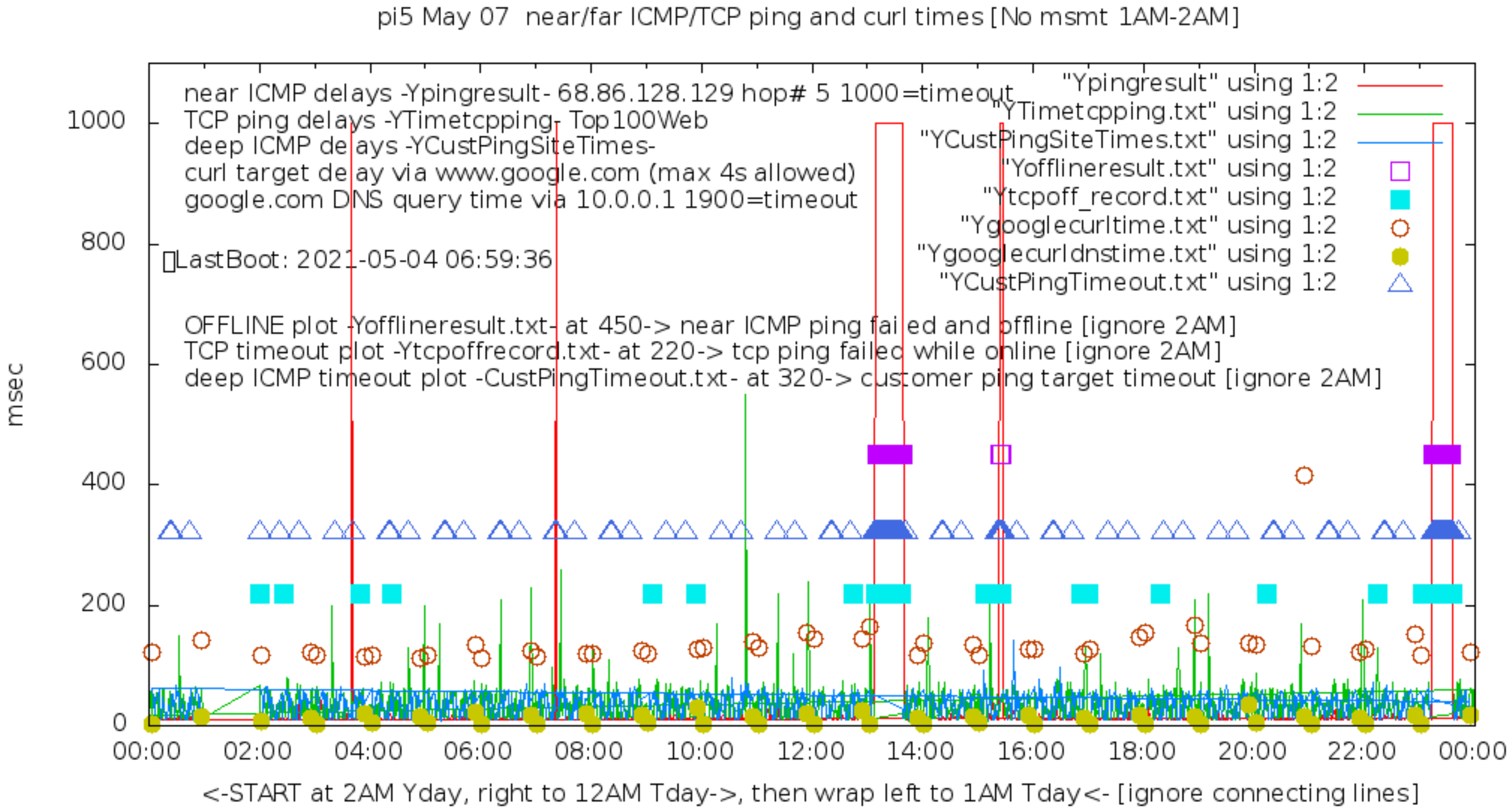
g. Internet scan for open ports on Saturday. [very important to detect external susceptibility to Internet intrustion]

h. The ability to generate a "real time" plot showing the day performance to the time you click. Really neat feature!

i. Many more tidbits of info/configuration are available at the rpi web page. Completely safe - it is on your home network!

7. Short course on interpreting plots

The daily morning email has a lot of info about your ISP connection [you can see an example at the imonitorg.com web page], and your local network for the previous day, but the attached plot may be the best -visual- indication as to what is going on. It represents "performance monitoring" of your connection for the previous day. Here is a quick interpretation of pi5 - Kristina in Denver for May 7. Connection was very good up until about 1PM, when she completely lost connectivity for about 40 minutes, again at 3:15PM and at 11:15PM. You can see the ICMP delay pegged at 1000ms [timeouts], the blue flags for hard offline, the grey flags for tcp timeouts, and the blue triangles for customer ping timeouts stacked there. All four indicate a hard timeout during those times.



Notice the points [as lines] plotted: [thanks to wifey for color interpretation. Note: YOUR plot colors may differ!] The plot STARTS at 02:00 yesterday, goes to 00:00 this morning, and then wraps to 01:00 for today.

a. The red continuous line are the "near" ICMP ping delays to the [(automically or manually) selectable] ping target, typically 5 hops into the Internet, [tho Niel -pi24- as another reference, is 8.8.8.8 since his hops are not pingable]. These pings use IP address only -thus no DNS query- and they are triggered by an hourly cron file. They should plot as a random statistical value around the pingtime average, and are generated every 1 minute. You can see the congestion from 3:30PM to 5PM as there are MANY ping timeouts, represented by the 1000 msec delay. There are additional congested periods around 3:30AM, 7:30AM, and 3:30PM.

b. The green continuous line are the TCP ping delays to a round robin of the top 100 web sites [in the US]. These run 24/7 [not called via cron], and invoke a DNS query for each ping. These are typically to the nearest CDN [content distribution network], so delays are typically small, almost as small as the ICMP ping delays. Any TCP timeouts are also flagged by the green boxes at the 220 msec time.

c. The blue ping continuous line are the "far" ICMP ping delays. These are only plotted on the managed pis [pi1-30], and they are a collection of the "near" ping targets of the other managed pis. So they represent a ping, typically deeper into the Internet, and they do not do a DNS query. Some of these are not pingable from other ISPs, perfectly normal.

These three lines are typically merged into indiscernability on the plot for a well-functioning access -such as above from 2AM to 3PM and 5PM to 12AM -this is normal. You can always zoom into this plot for details, or go to the actual data file for details. There are five other values plotted using solid box/triangle/circle:

d. The purple boxes represent actual "offlines" experienced by the rpi. This is a matter of definition.... For the rpi, an "offline" is declared if a tcp timeout occurs DURING an ICMP ping timeout, so think of two sliding second long windows [ping timeout value] passing each other in a 1 minute interval. On a statistically multiplexed connection, "offline" is a matter of definition, and this interpretation is my own. Notice the "offline" declarations at 7:30AM, 1PM and 2PM, tho notably NOT during the congestion around 4PM. *These are flagged at the 450ms delay time for convenience -this does not mean that is the actual* ***delay*** *-it is just a* ***flag*** *indicating offline.*

e. The teal boxes represent tcp timeouts. *Again, these are flagged at the 220 msec delay*. A smattering of these is very little of a problem.... CDNs may actually switch their actual host from local to very far away, and actually appear as a timeout if the near one is under congestion/failure. I have seen CDN for some sites switch from Denver to Thailand!!

f. The brown open ping circles represent a "web page access" to the default target, a much higher level delay measure. It is actually a "curl" to a definable target, tho it defaults to www.google.com. In the case of pi24 here, *Niel's ISP Tmobile actually blocks curls*, so we define the target as his local router!!! This is why I had to change the curl target to be configurable. These only occur twice per hour.

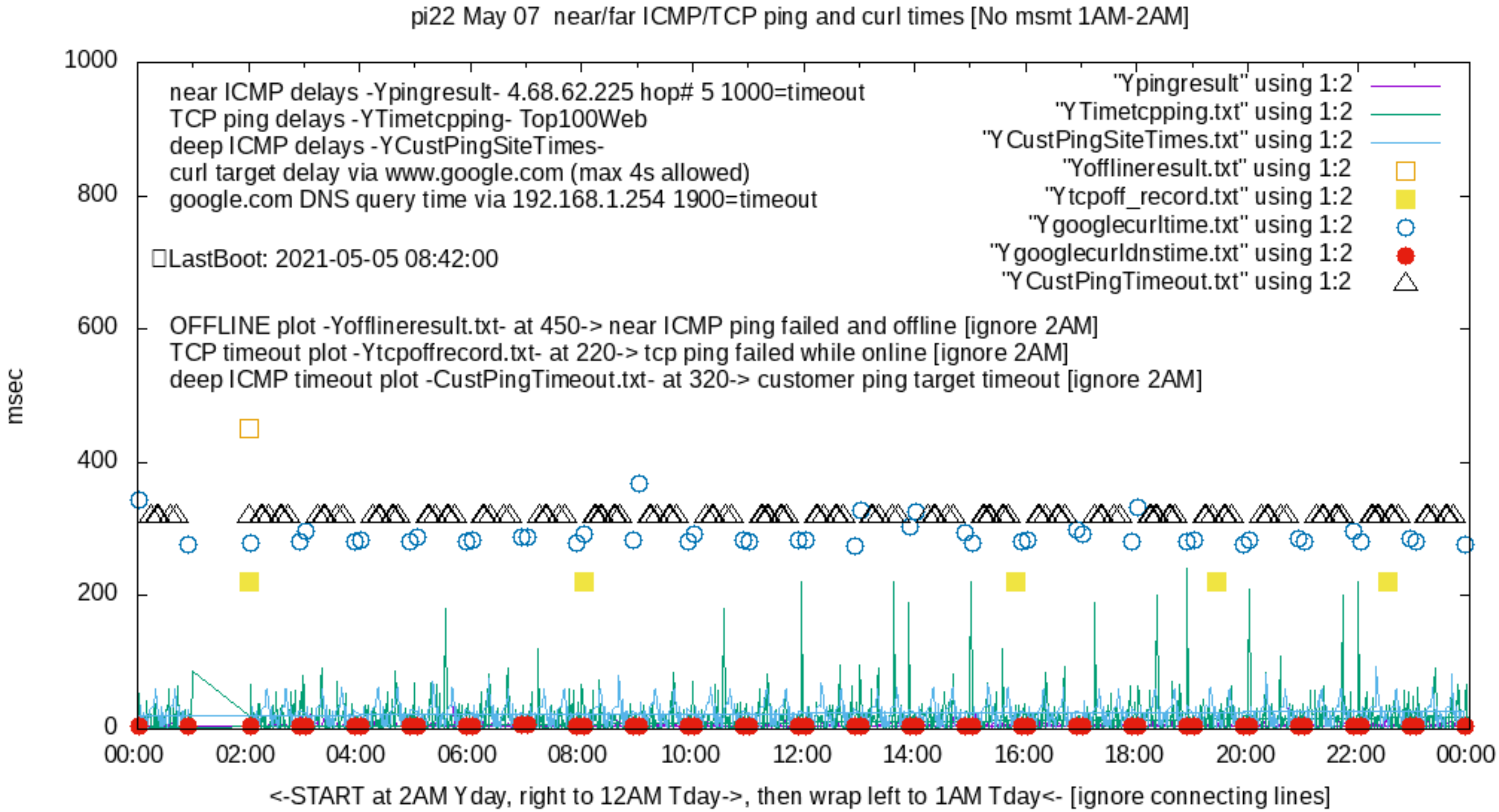
g. The solid green circles represent a DNS query delay, typically to your local router, so it should be the shortest of all the delays -attempted twice per hour. Almost all ISP routers do DNS caching, so your actual router responds to DNS queries. The router may have to go get the answer from the Internet if it is not "cached" and has not "timed out." You can actually see the router delay every other query as it goes to the Internet. This depends on the DNS cache time in the router. Several ISP routers, however simply pass these requests on to an Internet DNS server -they are a DNS relay instead of a cache. The rpi uses the DNS server assigned by your router via DHCP, and it is not configurable as such so as to represent a "normal" gadget on your network. You are always free to statically assign a DNS server in your PC, or maybe even in your router. And of course, the FFOX, Edge and Safari browsers do their own DNS query these days using "DNS over HTTPS" - so these DNS queries are not seen by the rpi.

h. The blue triangles represent customer ping timeouts. These occur much more frequently and should not be a concern. Many of these IPs, being almost "inside" the ISP network, may not be -always- pingable from remote ISPs. So this is just additional information to gauge connectivity. *These are flagged at the 320 ms delay time for convenience.*

The five sold box/triangle/circle are much more of a higher level feel for the ISP performance, which is why they are "flagged" on the plot at a fixed [delay] value, rather than delay plotted.

Here is Charley's plot pi22 from May 7: Charley has an almost "perfect" connection with 300Mbs Down/Up speeds on an ATT fiber in Atlanta. Notice his statistical, indiscernible scattering of the near ICMP, tcp and customerping lines around 20-30ms delay. Even his connection suffers the occasional tcp timeout [yellow flags], and the spate of deep ICMP customer ping timeouts [black triangles] -those IPs are not pingable from his IP. Notice however that his web draw [curl -blue circles] to www.google.com [~280ms] is much slower than Kristina's above [~120ms] -he must be further [router-wise] from the nearest google CDN? But it is the consistency which is important.

NOTE:different color scheme [depends on your pi config]: this is about as good as it gets.



It is very instructive to compare these plots at https://imonitorg.com/customerplots/rtcustomerplots/ [this is a directory listing] ---use the "combined" name key. They span technologies and ISPs across the country, from DSL, VDSL, fiber, cable, WADSL, cellular. You can compare the delay archive plots and the speedtest archives on the page as well.

As always, I especially appreciate my "guinea pig" volunteers in this project. We have had a good time quantifying our ISP performance and interpreting results and trying to improve the stats.

I look forward to reporting more pi0w information in the next newsletter.

John Loop

QuickManual.pdf
169K