

Imonitor Quick Guide [9-1-2021]

Installing the imonitor raspberry pi 3B[3B+] on your network, and running my custom scripts will give you wide-ranging and realtime monitoring of your local network and Internet performance, via a daily email status report and a webpage available on the raspberry pi 365/24/7

The imonitor will "come up running" and it is only necessary to set the time zone via the "raspi-config" and the email parameters via the rpi web page, if you desire email. It uses the normal pi user to run most of the scripts, as well as some root scripts. "Pihole" application is also included - point your DNS server to this pi and monitor all DNS activity.

1. Who should use an imonitor

Residential or small business Internet customers

Single NAT'd IP appearance on the Internet

Cable, ADSL, satellite, cellular, or fiber WAN interfaces with a LAN side ethernet or wifi access

Anybody with a single NAT'd IP appearance on the Internet who wants to monitor and gauge their Internet performance over long terms.

2. Access the raspberry pi [also referred to as rpi]

Plug the raspberry pi into an ethernet port on your Internet router, or a switch connected to it. The raspberry pi expects an IP address, gateway and DNS, just like any device that you add to your home network. You will have to find the address of the raspberry pi - usually by going to the router home page and looking for it. Once you have the IP address, just browse to the raspberry pi - this will be http only, not https, so you may have to make exceptions in the browser to allow the http. Once you have the web page, you can setup various parameters, tho it will work out of the box. The most important thing you can setup is the email configuration. The info will be copied to my server and night, and will be forwarded to the email configured in /root/DEFcustemail.txt.

Alternately, if you don't want to mess with ethernet you can connect a KVM to the raspberry pi [HDMI monitor, USB kbd/mouse] and login to the desktop. This is a standard distribution raspberry pi. The login is pi but the password is custom - you need to contact me for the password. Once on the desktop, you can setup a wifi connection - using the icon in the upper right. You can choose to use wifi only like this, or have the wifi in addition to the ethernet.

3. Setup raspberry pi interfaces - Ethernet and/or wifi

The "imonitor" is a generic raspberry pi 3B or 3B+ [4B coming] - the only thing different is all the scripts and cron entries to effect the network monitoring - these will run automatically on boot, once it is able to see the Internet and synchronize ntp clock service. You will login to the raspberry pi using the pi login, either via a KVM desktop, or via ssh to the user pi from another computer. The pi is useable as a normal raspberry pi in all respects. Just do not modify the scripts or cron files.

The imonitor expects to operate behind your Internet router on your private network in the same manner as one of your network devices. It will expect an IP address/gateway/DNS via your DHCP. It should not be connected directly to the Internet, as there is no firewall running. *Connect your ethernet and/or wifi interfaces as follows.*

Ethernet only. Plug the imonitor into your router or a switch on the same network as your router [or a router behind your Internet router]. Wifi networks are detected and scanned for SSID/Signal Level/Secured, but imonitor does not participate in wifi. Ping and TCP stats are performed via Ethernet only. No Wifi SSID/passwd needs to be provided.

Wifi only. Wifi SSID and passwd are needed. I can provision these via cmd line, or you can do it via connecting a KVM to the imonitor and doing it much like a Windows or MAC PC - there is a convenient wifi icon in the desktop upper right. Ping and TCP stats are performed over the wifi since the Ethernet is not connected.

Ethernet and wifi. Wifi SSID and passwd are needed. This provides the most complete testing. Ping and TCP stats are performed over the Ethernet to the Internet. Ping stats are performed over the wifi to your gateway only to gauge wifi network performance. [this mode may disappear in the future due to routers inconsistencies with wifi provisioning simultaneous with ethernet to a single host]

4. Configure imonitor options from the webpage:

- Control email options [YES, NO, OFF]

Set Customer email [where you want to receive status/alerts]

YES - daily status email, plus alerts:

IP address/DNS changes

Reboot [or power outage?]

Online/off Internet notification

Temperature alerts [if probe installed]

NO - Saturday email only [showing all days], alerts provided -as above

OFF - No email at all, no alerts. Only info is via webpage. I would not recommend this, as the email contains a lot of info not easily accessible via the web page.

Email capability will require [a TCP port] access to my management server on the Internet in order to collect the local stats and scan your Internet connection -and then email you. As indicated above, this can be disabled. It is near impossible to configure email capability on each imonitor given the different ISP requirements on email sourcing.

Communication with the server is via ssh over a special port, and a “reverse ssh” established simultaneously to allow the server to communicate with the rpi. The mail “innards” are scp’d to the server who in turn emails the customer. Additional info, such as an Internet scan of the rpi appearance is performed and relayed in the email. Individual rpis will have a public/private RSA key pair, which the server will use to communicate with the server and vice versa.

It is also possible to simultaneously setup the gmail relay and use this to receive daily email status and plot. Alerts are not currently supported, but they are listed in the daily status. This functionality is primarily intended for the rpi in generic mode [see below].

Set gmail relay [where you can receive the daily email status] using rpi web page:

gmail relay enable state - YES or NO

gmail account - gmail account "username@gmail.com"

gmail authorization - gmail app password

ultimate email - ultimate destination email address

See this link for e.g. instructions: <https://johnloop.com/imonitor/gmailRelayInstructions.txt>

- Set Management Options [ON, TempOFF, OFF]

Management is necessary for the development and updating of the imonitor. However, development is at such a state [Aug 2019] that it can be released from active control. I will only request access occasionally to update, and you will have to enable this if you are running in STANDALONE mode. Otherwise I can manage independently. You can turn the email status completely off as well via the above options, in which case your information is only accessible via the imonitor webpage. You must allow me to manage occasionally when I request if you are a "guinea pig." If you hesitant about allowing a device on your network, then turn the mgmt off [tho the IOT devices you put on your network are much more unknown in their behavior than this device!]

Disabling the mgmt interface has no effect on the Rpi operation. It just cuts off access for my updating and testing, which is discouraged during the development stage.

ON - Allow update and management 24/7 of the device

Temporarily OFF - Turn off update and management until next 1AM

STANDALONE - Disable update and management. Daily email and alerts are still supported as long as "DEFdailyemail.txt=YES. You will be able to acquire updates via instructions from me.

In any wide scale “deployment” of this device, the management will be set to OFF which will mean the only way to collect the data is to go to the web page. This is because the current implementation is not

scalable to large numbers unless a server on -e.g.- AWS is implemented to handle the uploads/scans/mailings. A better authorization scheme may be needed as well.

-Management versions

1. full mgmt: DEFsa.txt=OFF, DEFdailyemail.txt=YES, piX <-> server [pi reports in, server can access pi for updates/debugging, relay email]
2. partial mgmt: DEFsa.txt=ON, DEFdailyemail.txt=YES or NO piX -> server [pi reports in, server can relay email, but not access pi] [DEFdailyemail.txt=NO means sat email]
3. no mgmt: DEFsa.txt=ON, DEFdailyemail.txt=OFF piX ->block<- server [pi does not report in, server cannot access pi]

#1 and #2 and #3 piX has the public key of my server and can reach it. My server has enabled the piX public key. ssh/scp will work if invoked from user pi. DEFsa.txt=ON disables the ability of my server to reach the pi [no reverse ssh channel established]

4. Generic: essentially 3, **but public key of my server removed from pi**, and server does not have pi public key. Pi cannot reach server, and server cannot reach pi. No server resources used. ssh/scp will not work between them.

- Configure “near” ICMP Ping target, and "LOCK" or "AUTO"

Ping target temporarily settable, but it reverts to automatic mode next 2AM. A "lock" option on the Icmp ping target is available to override this. It is fixed until manually returned to "auto. "

The timeout is 1000 msec. Automatic mode configures the ping target as the closest pingable hop starting at hop 5 and counting down. It uses **IP address only** to forego use of DNS. It uses a close target to gauge local ISP performance, independent of DNS and Internet-at-large. ICMP echo request packets [UDP only] are used. This near ICMP ping will record outages.

It is also possible to set the hop start used for the ping determination to further allow customization. This can be 5,4,3, or 2, but not 1. Sometimes the auto algorithm settles on a ping target[s] that can become very unreliable. We need to find a reliable near ICMP ping target.

- No configuration is necessary for “deep” ICMP ping

A third ping type of ping, using ICMP, uses the ping targets of the other rpi customers. This guarantees ping targets “deep” into the Internet for the other customers, unlike the “near” ICMP target configured at each customer, and even the TCP ping, which usually results in pinging the web site on the nearest CDN [Content Delivery Network] appearance. This ping list is update automatically every night from the mgmt server. No ping is attempted if the rpi is offline. The near ICMP ping is the only ping which “records” outages.

Operating in “Standalone” may disable the “deep” ICMP ping, since the targets are collected from the remaining rpi’s via the management server. However, managed rpis will have the key of the server, so the CustPingSites.txt list should be pulled each night from the server even if the rpi is in standalone "ON."

- Configure TCP target, and "LOCK" or "AUTO"

A "connect" is performed to determine online/offline status each minute. A tcp "ping" is performed to determine response times each minute. The Internet FQDN DNS name should be used to invoke DNS query mechanism. "www.google.com" or "www.msftncsi.com" is suggested for the FQDN. A "lock" or "auto" may be applied to the ping. The "auto" option uses the top 100 Web sites as TCP ping targets. The "lock" option uses the target as the TCP ping target. The TCP connect target remains fixed even with "auto" option. It uses a "tcp" target to better gauge larger Internet performance. It uses TCP half open exchange, sending a SYN, and if a SYN/ACK is received, returns a FIN/ACK. The TCP Ping is only attempted while online [Internet accessible].

- Configure curl of URL

Twice an hour a "curl" of a configurable URL is performed, and the time recorded. A "curl" is just a cmd line way of "browsing" - pulling down a web page. This response time is plotted on the daily plot with the three other measurements, or the "callable" plot. This scan represents the "highest level [from a protocol level]" scan performed. Only the index page is downloaded, not the images and links referenced in the index page.

In addition, the dns response time of a curl to www.google.com is recorded and plotted when you do a manual plot from the rpi web page. This normally uses the default gateway/router, since this is what is normally specified for the user [but not always]. It is thus a good measure of inside network performance of the router.

- Enable *Internal* scan of your network [default OFF, ON]

This is a scan conducted by the rpi on your internal private network. This scan result is kept locally and is not communicated off site. Linked in email. It can be especially important if you have wifi in a wifi maze of networks. It scans for vulnerabilities on your network hosts using linux "nmap." It discovers, **lists all hosts** and changes day/day on your internal network via IP address. There is a listing, including a historical listing of HOSTS/ports in "Data snapshots," complete report in "counts."

- Set Temperature Probe Up and Down email alerts

If temperature probe installed. 10 emails sent at 15 minute intervals if alert remains.

- Configure pihole

The rpi comes with pihole already installed. Confer <https://docs.pi-hole.net/> for a description of pihole. The Rpi web page has a link for the pihole administration page, and also links for the pihole log which is collected by the rpi.

Pihole expects a static IP address, and it must be set using either the pihole admin page, or going to /etc/pihole/setupVars.conf and setting it there [and rebooting]. You should also go into the admin page ->settings->conditional forwarding and set your network and router address. It is not necessary to use the pihole as a DHCP server.

If you wish to see DNS queries from the browser [chrome/FFOX etc], you will have to turn off DNS over HTTPS. The "DOH" is defaulty enabled as of 2021 in most browsers. Otherwise, record the log as without browser -which would show you the non-browser activity, and then turn off DOH to see additional browser activity.

- Additional configuration options

Route target for hop delineation.

The linux utility "nmap" is used to perform a scan of your local network. This is detailed on the rpi web page. A list of IP addresses, change of IP address, services, and change of services day over day is performed. This can be enabled/disabled on the rpi web page.

5. Email advantages/summary

The daily or weekly email is probably the easiest way to monitor performance and statistics of your Internet connection. I would not recommend turning the email off. You should at least receive the weekly email status reports. If you turn off email [see above], your only stats will be via the web page [see below]. The email will give direct links to Rpi web pages detailing info [you don't need to go looking for the info onthe web page!].

Email capability will require [TCP port 3313] access to my management server on the Internet in order to collect the local stats and scan your Internet connection -and then email you. As indicated above, this can be disabled. It is near impossible to configure email capability on each imonitor given the different ISP requirements on email sourcing.

Imonitor overall settings and interfaces participating [ethernet and/or wifi]

Internet IP address, ISP, DNS status, interface states, **plus http links to local info**

ICMP ping stats for yesterday, **plus http link to plot** -yesterday,today so far

TCP ping stats for yesterday, **plus http link to plot, plus archive of average**

Http link to Temperature **plot** for yesterday [if temp probe installed]

Online/offline stats since reboot, or first of month

Speedtests, performed at 3AM and 3PM [the same kind you do from your PC], **plus http link to speedtest history plot** <- you can see a history of your speedtests

Wifi scan of visible wifi networks [does not require interface participating with IP add]

Direct links to imonitor webpage, gateway, internal scans

Internet scan results, list of open/closed ports

Internal IP network devices, plus historical and daily added/subtracted notifications

6. Some advantages of using the imonitor webpage

The webpage is implemented on your local network only, and is completely safe. There is a link to it in the daily email, so it is easy to get to. Here is a link to a pdf of the current webpage

<https://johnloop.com/imonitor/RaspBerryPiWWW.pdf>

It gives all stats reported in the email, and is the way to configure your imonitor.

Perhaps the neatest thing is that you can request a "real time" plot – the same one that you get in the email, except it starts at 2AM and ends when you request the plot. You can also select a "ping blast" plot, where 60 pings are delivered to the ICMP ping target, and then plotted.

As of 9-1-2021, you can specify the start of the "real time" plot so that you can narrow in on problems. In addition there is a "hyperping" capability which triggers a more intense ping of 12/sec when the 1/min ping times out. If these "hyperpings" timeout, they will be designated by "ticks" on the plot ascending vertically above the minute they were launched. This gives a much greater feel about the network availability around the 1/min ping failure.

There is no upload to a webserver in the Internet cloud to collect info [many similar services use a cloud account and require you to have an account/login to see the info for your own local network]

The webpage is accessible even if the Internet is down, as long as your local network is OK.

The webpage is not loaded with widgets and gadgets, with background loading of dozens [hundreds?] of websites and cookies. It is a very simple implementation showing stats and enabling configuration. There is only one figure included, and no scripting other than for alerts, and to allow you to set imonitor parameters.

The webpage will show dated ping times, plus giving a link to the plots. Plus:

1 year archive of all plots and speedtests available, services and port changes on your network, plus the daily emails.

1 year archive [plus plot] of Internet offline dates and times.

On the pi3B+ [and 4B eventually] the "pi-hole" app is installed, and is linked from the main page. Info is here <https://pi-hole.net>

7. Advantages of server imonitor.org.com

This serves as a reference for the rpi and its functionality. There are links to various items, including a page where you can see representative ping plots from other customers, and hints to interpret your statistics. There are also links to the newsletters published.

8. Some advantages of using the imonitor on your network.

The ping plots are particularly useful for quick comparisons of your network performance. You can quickly scroll thru days of performance in the archive window on the webpage. The same goes for temperature monitoring, if you have a probe. A sample ping plot and temperature plot are included.

Archiving of all data, emails and plots, boot times, IP address records, for at least 1 year.

Saturday scan of your Internet presence for vulnerabilities, and attach to email

Daily scan of your internal network for vulnerabilities [if scan enabled]

Daily scan of wifi maze, listing all visible networks and characteristics, every 30 min

The ethernet [or default ifce] ping tests will probe into Internet. The wifi ping tests probe your local network [as well as Internet if you are wifi only]

Listing of your local network hosts and svcs, plus notification of changes [detected at 7PM].

9. Special Considerations

On a boot/reboot, the system clock may be wildly off until the Internet is acquired and ntp can sync the clock [depends on how long the rpi was off the Internet]. The rpi and the modem/router should use a UPC for reliable stats. The ping target is calculated at 12:55, so restarting the rpi at any other time will use the ping target of the previous boot. If the rpi wants to use the wifi, the SSID/key must be entered, either via connecting a KVM, or by modifying /etc/wpa_supplicant/wpa_supplicant.conf

The raspberry will operate with any IP address it is given via DHCP, but the scripts may need an overnite to update all the links when the local IP changes.

If the rpi changes IP address, the pihole must be reconfigured.

If you expect off-network unsolicited SYN's to the pi, you should "echo OFF > /root/DEFunsolicitedSYN.txt" Otherwise the mail1 file will fill up with alerts. The pi performs an unsolicited SYN detect by default.

11. For Information: <https://imonitor.org.com>

John D. Loop pccitizen@gmail.com or jdloop@johnloop.com

This is a sample combined plot. Individual ICMP and TCP ping plots are also available via the web page. A sample Combined ICMP/TCP ping plot is shown here. It shows the values collected during the day, and the pi going offline at 6:00PM till 1AM the following day. The scripts and presentation are the sole property of John Loop.

12. Converting to a "managed" rpi

If you choose to operate in standalone mode, it is still possible to convert the standalone rpi into a managed rpi by turning "standalone" into "OFF." The server has the public key of the imonitor rpis. In this manner, I will be able to access the rpi for updates and monitor as I develop it further. Standalone "on" mode still allows the user to participate in the daily email and alerts.

13. Using pihole

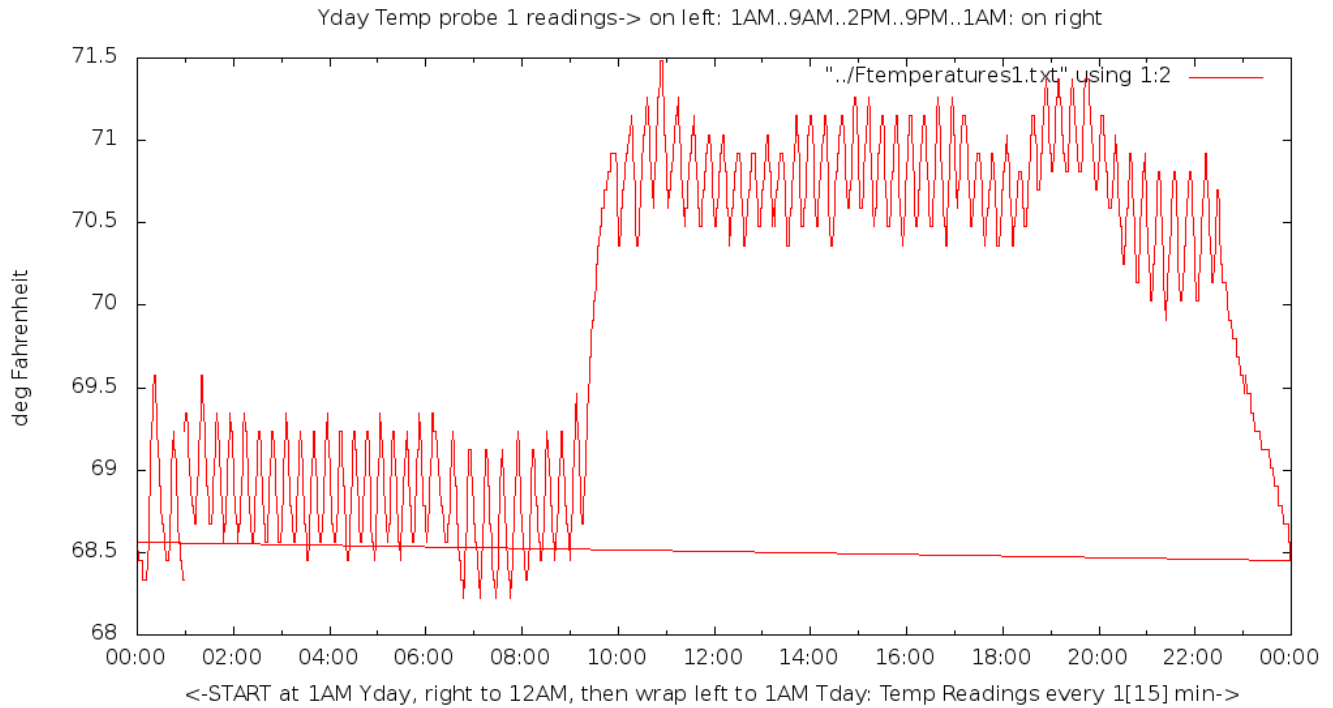
Pihole is installed on all rpis. It is accessed via a link on the main rpi web page, or via http://RPI_IPaddress/admin/index.php. Pihole provides a way to monitor all DNS activity on your local network. You can configure individual clients on your network to use the rpi as your DNS server, and all DNS requests will be routed via the pihole. Pihole was originally intended to be used to filter DNS requests to block ads, but it is implemented here merely to monitor the DNS. You may still configure with the adlist servers to do the blocking. The docs are <https://docs.pihole.net>.

You can monitor the pihole log on the rpi web page, as it is updated at 5 minute intervals, and also see Yesterday's pihole log. Pihole was originally meant to be used with filter lists to filter out ad/malicious web addresses. As implemented on the rpi, there is no filtering, but it can be added to the pihole in the normal way. These DNS queries are archived as well.

14. The plots

One of the neatest things you have access to is the daily [delivered via email if it is setup, otherwise available on the web page], and on-call real time plots of performance. Here is a sample plot received in the daily email. There are also two on-demand plots you can call from the rpi web page.

The first plot is a 24 hour temperature plot, taken at 1 minute intervals. This is available if you have the temperature probe installed and enabled. Contact me for details.



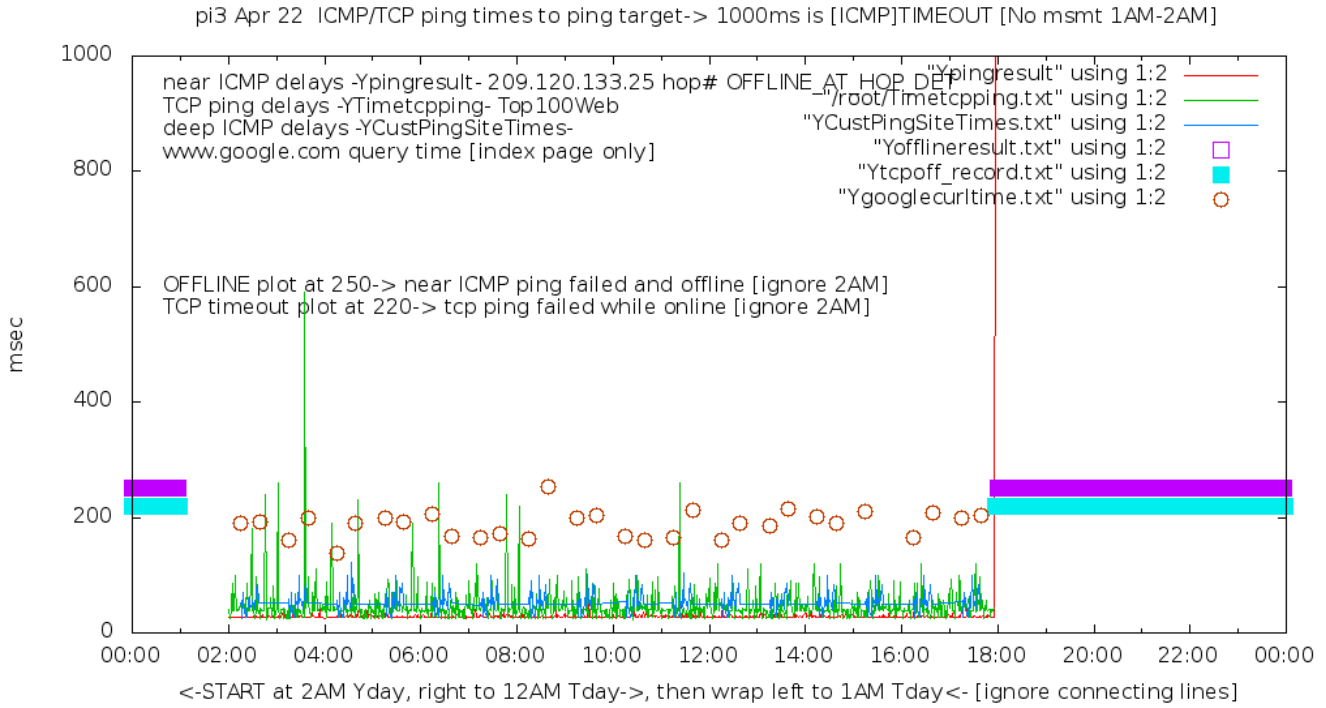
The second plot is a ping plot, using 3 different pings, explained below.

Individual ICMP and TCP ping plots are also available on the rpi web page. A sample Combined ICMP/TCP ping plot is shown here – this is the one received in the daily email. The explanation of the plot is in the next section.

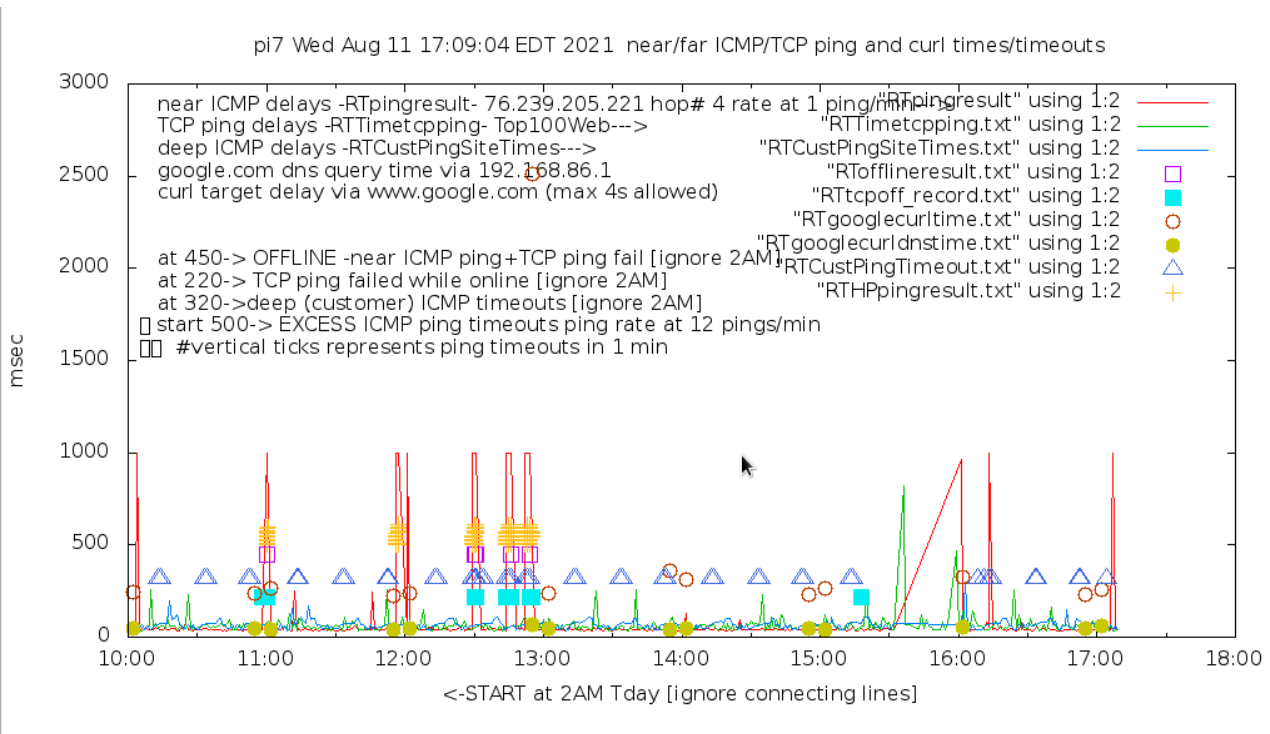
There are two callable plots available on the raspberry pi web page:

http://RPI_LocalIP/#snapshots Push the "PLOTIT" button and then the "wait for timer"

1. The combined plot, the same received in the daily email, except it represents the plot from 2AM until the time it is requested.
2. A "ping blast" plot, which represents a ping blast of 60 ICMP echo requests to the ICMP target in the space of 60 minutes. This is only performed when requested.



The third plot is the current incarnation [8-2021] showing additional info. Somebody is having a bad day!.



15. Ping Plot explanation

There are 3 main LINE plots: The ping delays of a close router [pingresult], the TCP delays of top 100 web sites [Timetcping], and the ping delays of a far-away router [CustPingSites]. These are the three colored lines. The close ping delays and the TCP delays are every minute for 23 hours [2AM till next 1AM], the far-away ping delays are about 20 minutes in the middle of the hour [there are straight lines connecting these]. Typically, the close ping delays should be less than the TCP delays and be fairly constant; the TCP delays will vary widely, normally between 20-100msec. The TCP delays will typically be to the nearest Content Distribution Network (CDN) which host most of the major web sites. The far ping delays may be the longest, since they are the ping targets of the other customers.

The fourth and fifth plots are the points that represent the twice hourly fetch of www.google.com, the curl and the dns query. This will typically have the longest delay. DNS name resolution will have to be performed for this, and for the TCP delays. The ping delays do not need a DNS name resolution.

The sixth and seventh and eighth "plot" are actually an overlay on the plots which will represent offline times experienced, TCP and customer (deep) ICMP timeouts, but still on-line. These will appear as bars when there are extended periods of offline state, or multiple TCP ping failures. These are plotted at the 250 and 220 msec delay times.

Added in Aug 2021 is the "hyperping" plot. This will be ticks on the plot which designate ping timeouts at 12/min rate, invoked when the 1/min ping rate fails.

Here is a partial day plot created by pushing the "plotit" button, showing "deep ICMP" customerping plotting:

