# Vbox ImonitorG Quick Guide [4-1-2023]

### Installing the “imonitorg” in your Oracle VirtualBox will give you wide-ranging and near realtime monitoring of your local network and Internet performance, via a webpage available on the vbox 365/24/7.

The vbox imonitorg will "come up running" and it is only necessary to set the time zone via ubuntu desktop/cmd line, and the email config via the vbox web page, if you desire email. It uses the "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. [pihole app install is currently in beta] The "imonitorg" scripts were originally developed on raspberry pi 3B and 3b+, and the scripts are transferred/altered to run on an ubuntu desktop OS, running on a virtual hyperviser such as Oracle VirtualBox. The distribution "image" is an "ova" - open virtual archive format.

## *1. Who should use an vbox imonitorg*

### Residential or small business Internet customers

Any processor capable of running a hyperviser such as Oracle VirtualBox should be capable of running the "ova" image. It is configured for 4 processors, 4GB RAM, and 32GB of disk space, tho these can be altered after importing the ova "appliance." The network adapter should be adjusted in the VirtualBox setting to "bridged" and the host OS network adapter selected. You can adjust the number of processors to fewer.

Any processor NAT'd to the Internet who wants to monitor and gauge their Internet performance over long terms should be able to use this. The Ubuntu virtual appliance itself does not have a firewall or selinux installed, thus it relies on the host OS being NAT'd.

## *2. Setup and Access the vbox*

Install the vbox "ova" in the normal way. This version uses Oracle VirtualBox as the hypervisor, tho I understand the "ova" image may be used on other hypervisors [I have not tested this]. Select the network adapter of the host OS and select "bridged." This allow the vbox to access your main network [or whatever network the host resides on]. Alternatively, you may select "NAT" to isolate the vbox from your main network. The vbox expects an IP address, gateway and DNS, just like any device that you add to your home network. You should assign this to be static via your DHCP server [normal dynamic is OK, but the stats will appear bogus and need "rejggering" once the scripts work their way "thru" the new IP assignment]. Once you have the IP address, just browse to the vbox - this will be htttp 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. This will use gmail as a relay [you can send

to the gmail address as well]. Of course you need a gmail account to do this, and you need to set up 2FA on gmail.

The OS is a standard distribution desktop ubuntu 22.04.2. The login is pi and the password is "raspberry." There is only one network adapter on the ubuntu OS, and this is virtual to the host network adapter, which can be wifi or ethernet. On the "vbox" there is no distinction between ethernet and wifi.

You will definitely want to set the TZ if you are not on the US East Time. Access the ubuntu in the normal way [ssh or vbox desktop on the host machine] and the cmd line or desktop in the normal manner and run to set the TZ and locale if you are not US.

# *3. Setup vbox interface*

The "imonitorg" was originally an image created for a generic raspberry pi 3B or 3B+. Many scripts have been added 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 vbox using the pi login, either via the desktop in the VirtualBox app on the host OS, or via ssh to the user pi from another computer. Do not modify the pi or root scripts or cron files.

The imonitorg 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 DHCP. It should not be connected directly to the Internet, as there is no firewall running.

# *4. Configure vbox imonitorg options from the webpage:*

## - Email setup

On this generic vbox imonitorg, it is possible to receive a daily status email by using the relay capability of gmail for user accounts. Your gmail account must be set for 2FA, and you must obtain a 16 byte key to use as the authorization string,

**Set gmail relay** [where you can receive the daily email status] on the vbox web page:

**gmail relay enable state** - YES or NO

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

**gmail authorization** - gmail app password -16 byte key obtained on gmail site

**ultimate email** - ultimate destination email address[es]

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

## - Set Cloud Management Options

There are no cloud management options on the vbox imonitorg. It is completely standalone. The original raspberry pi's used a cloud server for monitoring/update as the scripts were developed. 25+ users across the US with different access technologies and ISPs were employed. It covered

cable/fiber/ADSL/WADSL/Satellite/StarLink and home networks from exceedingly simple to dozens of home network gadgets.

A user may login as "pi" and perform operations, but he must be careful. All monitoring scripts run as user pi or as user root. He can create a new user and use that login for personal projects. The easiest "monitoring" may be just a browser open on the host OS pointed to the ubuntu vbox.

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

Ping target is 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. " "LOCK" is the default operation.

The timeout value is fixed at 1000 msec. AUTO mode configures the ping target as the closest pingable hop starting at hop [5,4,3,2 -configurable via the web page with 5 being default] and counting down. It uses **IP address only** to forego use of DNS. Thus it uses a close target to gauge local [near] ISP performance, independent of DNS and Internet-at-large. ICMP echo request packets [UDP only] are used. The timeout is set to 1 sec default. This near ICMP ping accumulates response times and will will probe for "prolonged" outage once a ping is missed.

As mentioned, it is 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. This can be adjusted once the ping behavior is noted after a few days.

## - “Deep” ICMP ping configuration

There is no “deep” ICMP target for the vbox imonitorg "out of the box." For the imonitor mode, these targets were the collection of the near ICMP targets of the other customers, automatically gathered and distributed to give a feel for "the Internet at large."

However, it is possible to place a file "CustPingSites.newtxt" in the /home/pi/tests/customerpings/ directory, and the pi will perform deep ICMP ping for one day starting at 2AM and ending at 1AM. This file should contain an IP address on each line. If you want the ping to be repeated, make a cron file to reload the file each day before 12AM. This will show up on the "real time" and the daily plots as a third line plot.

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

A TCP "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 is used to invoke the 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 [as of spring 2020]. The "LOCK" option uses the target as the TCP ping target. The "foundation" 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]. Care should be exercised in interpreting the TCP ping data. The top 100 web sites are largely implemented on local CDN sites.

As of spring 2022, the top100 web site listing uses "naked" domains. Occasionally, it is necessary to convert the "naked" domain, such as "google.com" to a valid FQDN such as "www.google.com." This occurs when a domain subscribes to a CDN, which requires a valid domain for CNAME. You can actually edit the /root/Top100WebSites.txt file to correct this problem. I have had to do this once. You can see when this problem occurs because the tcp ping timeout will appear periodic in the plot.

The /root/Top100WebSites.txt file is for US. You can modify this file, or reconstruct it in the same format for different countries [you can eliminate the third column]. It must contain exactly 100 lines.

"AUTO" is the default setting.

## - Configure curl of URL

Twice an hour, a “curl” of a configurable URL is performed, and the response 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 or the "realtime" plot with the three other measurements. 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 query response time for www.google.com is recorded and plotted. This is normally done to your router, as long as it caches or proxies DNS requests. The raspberry pi checks this, and reverts to 8.8.8.8 if the router does not perform caching/proxying.

ISPs will sometimes force the router to use their own DNS, such as comcast often does with 75.75.75.75. It is not possible for the router to override this -usually. The DNS server used for the DNS query is noted in the daily plot. Most often it is your own router.

The vbox implementation of imonitorg uses the latest pihole 5.15. As of 4-1-2023 this is experimental, and it is not yet understood exactly how the vbox pihole deals with the DNS. The vbox scripts use the router deterministically to do the DNS queries to check the router response time, so hopefully this bypasses the pihole complications. None of the block lists possible using pihole are implemented. Pihole is only used to give access to the queries. You can point a DNS client to the vbox imonitorg pihole and record the DNS queries, revealing much more detail about your PC.

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

This is a scan conducted by the vbox imonitorg on the connected [hopefully bridged] network. It can be especially important if your hosts OS is running 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.” These stats are available on the vbox webpage. There is an algorithm which spans a week to detect "new [never been on your network before]," "gone [it was previously on your network, but disappeared. This lasts for two scans]", and "persistent [this host has been on your network 10 or the last 12 scans]." This algorithm normally runs

twice per day, at 6PM and 1AM [busy and not busy]. It is useful to detect transient hosts and permanent hosts. This is actually configurable by changing the "findhosts" schedules in the pi crontab.

### - Pihole configuration and use

The vbox imonitorg comes with pihole installed. Confer https://docs.pi-hole.net/ for a description of pihole. The vbox web page has a link for the pihole administration page, and also links for the pihole log which is collected by the rpi. [as of 4-1-2023 this admin link does not work]

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.

### - Addional configuration options

Route target for hop delineation. This is a far end location such as 222.1.1.1 [Japan], or 90.1.1.1 [France] to control direction of the packets many hops from your router. This may not have an effect if the same 5 routers are encountered in your path for any destination. Other customers are but a few hops away from the backbone where it will make a difference.

## *5. Email advantages/summary*

There is a daily status email available by using your gmail account as a relay [see above]. It includes the daily plots, and a list of numerous network statistics.

## *6. Some advantages of using the imonitorg webpage*

The vbox webpage is implemented on your local network only, and is completely safe. There is no cloud server with all your data that you have to access!

It gives all stats reported in the email [comparing it to the “imonitor”], and is the way to configure your imonitorg. Here is a link to a pdf of the current webpage:
https://johnloop.com/imonitor/RaspBerryPiWWW.pdf

Perhaps the neatest thing is that you can display a “real time” plot – it starts at 2AM and ends when you request the plot. It is linked on a separate page called by this script. You must wait a minute for it. You can also select a "ping blast" plot, where 60 pings are delivered to the ICMP ping target, and then plotted.

You can also force plots at any time, and 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

6/sec when the 1/min ICMP pings time out. If these "hyperpings" timeout, they will 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 ICMP 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.

As of August 2022, the vbox imonitorg provides near-realttime plotting of the performance. There is a link at the top of the main vbox webpage. Clicking this link will open a new tab on your browser which will be updated every 5 minutes with the current plot. You can still do a custom plot from the main vbox webpage, which is linked from this page [click it and refresh to preserve the plot, otherwise it will be overwritten with the next auto update]. You can also manually change the update interval to every minute -instructions are on the actual webpage.

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 [to be added 4-1-2023] and no scripting other than for alerts, and to allow you to set imonitorg parameters. The "alerts" were originally configured for the imonitor [managed version] and generated a file to be discovered by the management server and emailed to the user. There is no such facility on the vbox imonitorg, but the alerts "accumulate" in the "mail1" file which is visible on the vbox or via the daily mail if setup.

The vbox 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.

The "pi-hole" app is installed, and is linked from the main page. Info is here https://pi-hole.net

## *7. Advantages of mgmt server imonitorg.com*

There is absolutely no contact with this server for the vbox imonitorg, tho it serves as a knowledge base and reference for the project. The server was used in the development phase, where 25+ users/friends across the US allowed me to test these scripts on varying situations/homes/networks/ISPs using a dedicated raspberry pi3 3B or 3B+.

## *8. Some advantages of using the vbox imonitorg on your network.*

The ping plots are particularly useful for quick comparisons of your network longer term performance. You can quickly scroll thru days of performance in the archive window on the vbox webpage. The same goes for many other plots and stats.

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

Daily scan of your home network for open ports and services [if scan enabled]

The ethernet [or default ifce] ping tests will probe into Internet.

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

DNS tests - DNS change alerts.

Browser tab showing near-realtime performance plot.

It is hoped to add the twice-daily speedtest measurements using the ookla speedtest CLI, but as of 4-1-2023 this is still in testing phase. The plots and scripts are all setup for this, but is not displayed at present.

# 9. Definition variables [settable via sudo to root]

These variables are located in /root and are set by sudo su – from the pi login. These can be changed by the imonitorg customer as indicated below, either via directly setting them via an ssh session, or via the rpi web page. They are not normally accessed except in special circumstances. Most configurable parameters are accessible on the vbox imonitorg web page.

1. DEFpi.txt -this is a null file for imonitorg.

2. DEFpingtarget.txt -this defines the near ICMP ping target, auto determined every hour unless it is locked via DEFpinglock.txt. CommToServer picks it up from localDEFpingtarget.txt every hour. Settable on the vbox web page.

3. DEFconnecttarget.txt - this defines the connection target, currently “www.google.com”; “www.msftncsi.com” is another good one - used by Microsoft to determine network connectivity.

4. Not used

5. DEFmgmtserver.txt – this is not used by the vbox imonitorg.

6. DEFinterval.txt - not used

7. DEFmgmt.txt - this is not used by vbox imonitorg.

8. DEFdnspull.txt – this defines where to get my IP address from. Currently “myip.opendns.com” This is hardcoded in the script. "o-o.myaddr.l.google.com" is also used. **Should NOT be changed**

9. DEFcustemail.txt -this is not used by the vbox imonitorg.

10. DEFmgmtemail.txt -this is not used by the vbox imonitorg.

11. DEFtimeoutinterval.txt - This defines the ping timeout interval, in msec, from 1000 to 15000. Currently “1000" is default for ping and is not changeable.

12. DEFrealrouter.txt -this file exists only if the vbox/host OS is behind an internal router, and is the internal IP address of the ***Internet*** router. Can test for existence of this file to test if behind internal router. **The customer must set this variable.**

13. DEFixc.txt -traceroute destination  222.1.1.1 points to Japan, 90.1.1.1 points to France.  It is really intended as a route eventual destination for "traceroute" even tho only the first hops are used.

14. DEFtemp1sensor.txt -not used by vbox imonitorg

15. DEFtemp1downlimit.txt  -not used by vbox imonitorg

16. DEFtemp1uplimit.txt -not used by vbox imonitorg

The DEFtemp variables are not used for vbox imonitorg.  The original raspberry pi could add temp thermometers and samples were taken and plotted.

17. DEFemailforIPchange.txt – this is not used for the vbox imonitorg.

18. DEFsa.txt – this is not used by the vbox imonitorg.  It is set to ON, "standalone."

19. DEFconfig.txt -not used by vbox imonitorg

20. DEFgmailENABLE.txt  - enable email relay via your gmail account.  Default NO

21. DEFgmailUSER.txt  - gmail user account to authenticate to for relay

22. DEFgmailAUTH.txt - gmail app password used with DEFgmailUSER.txt

23. DEFgmailULTIMATE.txt - ultimate email destination via gmail relay

The DEFgmail*.txt variables can be set from the web page.

24. not used

25. DEFpinglock.txt  AUTO or LOCK; "LOCK" locks value, "AUTO" lets script determine it automatically each hour for the next hour.  This can be set on the rpi web page.

26. DEFhop.txt 5,4,3,2,1  This represents the hope to start at to check for near ICMP ping target.  it is decremented until "2" to find a pingable near target.  Otherwise it is set to 1.1.1.1

27. DEFscan.txt  OFF or ON --internal nmap scan of customer network; default OFF.  This can be set on the vbox imonitorg web page.  Performed once each day.

28. DEFdailyemail.txt YES or NO or OFF – this is not used by vbox imonitorg.  It is set to OFF.  It was a separate mechanism to deliver mail in the development phase.  Separate from the gmail relay capability.

29. DEFtcppinglock.txt LOCK or AUTO.  LOCK means use the value entered in the form.  AUTO means use the top 100 web site list [as of spring 2020].  The value entered in the form is always used for the connect "test."  If you choose AUTO, it is only for the tcp ping testing.  Note that choosing "AUTO for the top 100 web, these will normally be sites on the nearest Content Distribution network [CDN].

30. DEFcreateRTplot.txt – set by entering the start time, and pushing the "PLOTIT" button on the vbox web page to create current plot. Cleared by script that does the plotting.  This variable is set via the vbox web page and checked every minute by CommToServer.  The plot will show the plot from the designated time to the time it is invoked.

31 DEFcreateMINplot.txt - set by pushing the ping blast "PLOTIT" button on the vbox web page to create ping blast plot.  60 pings in a minute to ICMP ping target.

32. DEFcustomerping.txt –  this is set to NO for the vbox imonitorg.

33. DEFversion.txt - set at image version creation.  Simple date.  Each execution of "/root/clean_piG_files_generic" is recorded here to signify "reset to factory default:."

34. DEFbootcurl.txt - not used by vbox imonitorg

36. DEFpiversion.txt  3B, 3B+  not used by vbox imonitorg

37. DEFimonitorversion.txt  date, such as 07/22/2020

38. DEFcurltarget.txt  -enter a URL for a favorite web site.  www,google.com is default.  This is used for the twice-hourly curl test.

39. DEFhop.txt -enter an ICMP auto ping hop start.  5,4,3, or 2, but not 1.  Default is 5.

# 10. Special Considerations

On a boot/reboot, for a raspberry bi, the system clock may be wildly off until the Internet is acquired and ntp can sync the clock.  The vbox host OS -and its vbox imonitorg appliance will likely have a much more reliabke clock.  Nevertheless, the host OS and the modem/router should use a UPC for reliable stats.  The ping target is recalculated each hour, so restarting the vbox at any other time will use the ping target of the previous hour.

There is a special script "clean_piG_files_generic" in /root which you can use to clean the vbox for initiation.  Beware, it wipes all history.

The vbox imonitorg will operate with any IP address it is given via DHCP, **but the scripts often need an overnite to update all the vbox webpae links when the local IP changes.  An entire day may be needed in some instances.  To determine hosts, a week will be needed to work the algorithm.** Assign a static IP to your vbox imonitorg to minimize these effects.

If the vbox changes IP address, the pihole must be reconfigured via /etc/pihole/setupVars.conf

# 11. For Information: https://imonitorg.com

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

Below are sample combined plots.  Individual ICMP and TCP ping plots are also available via the web page.  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

It is possible to convert the vbox imonitor into a managed vbox imonitorg via generating a key pair and sending me the public key, plus setting some of the DEF* variables above. It is not planned to do this for the vbox imonitorg at present, tho the underlying scripts are all there.

# 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 vbox 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 vbox 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 vbox, there are no ad filter lists used, but it can be added to the pihole in the normal way. These DNS queries are archived as well.

As of 4-1-2023 the pihole admin page is not accessible for reasons not yet clear. All the DNS logs are visible tho, and presented on the vbox webpage.

# 14. Plots

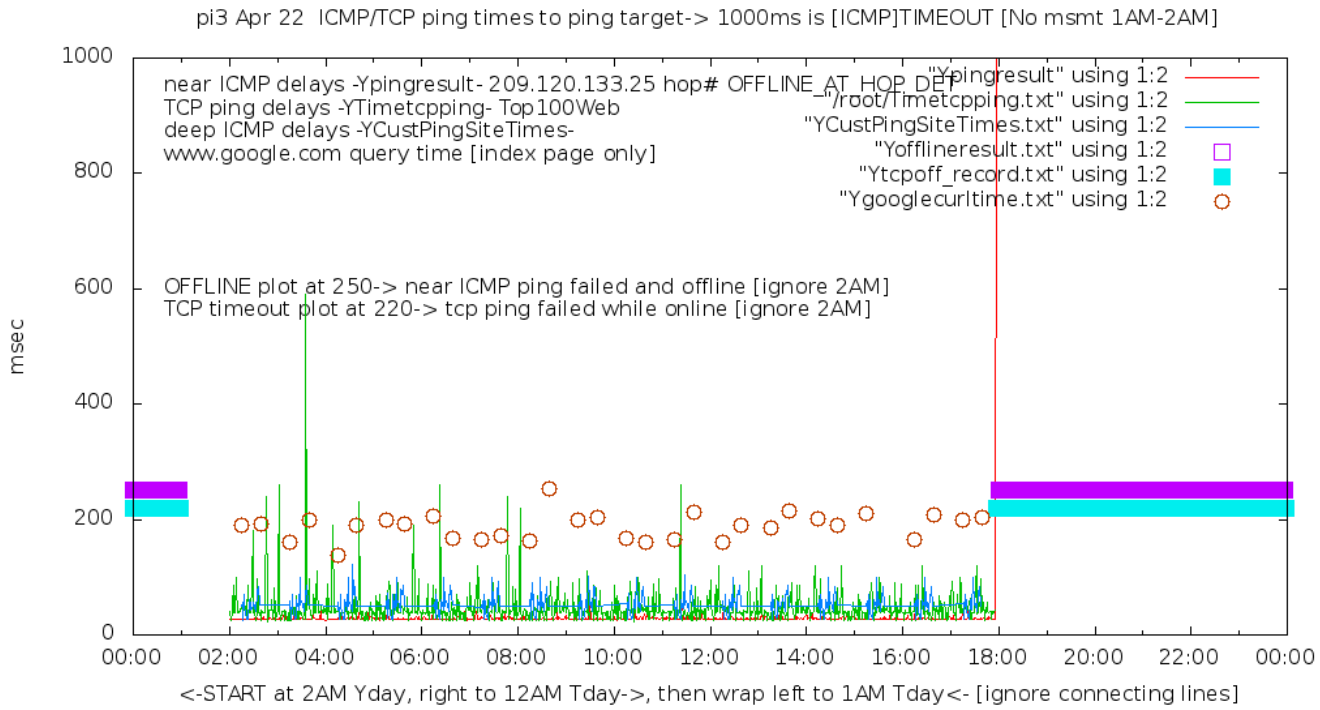
One of the neatest things you have access to is the daily [delivered via email if it is setup, otherwise available on the web page], and on-call real time plots of performance. Here are a few sample plots received in the daily email.

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

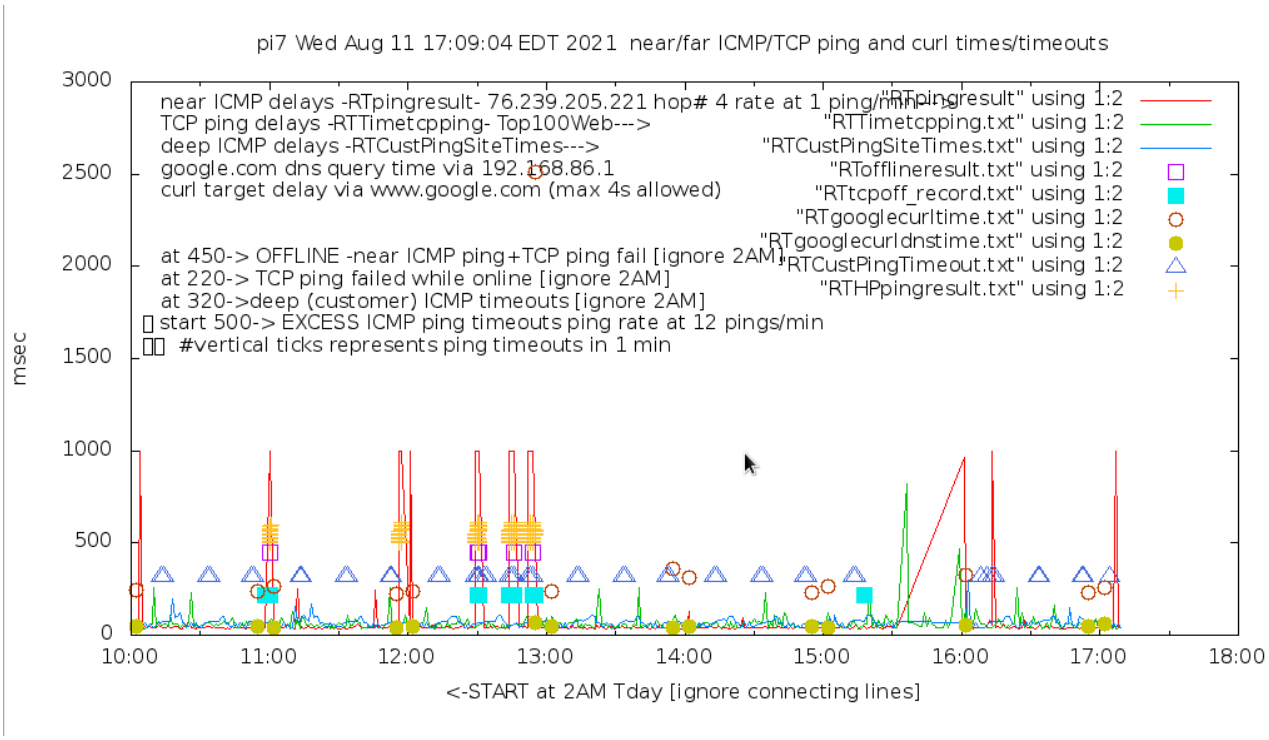
1. The combined plot, shown here, is the same received in the daily email, except it represents the plot from 2AM until the time it is requested.

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.

3. There is also a "near-realtime" plot of the performance linked on the main rpi page. This will update the plot every 5 minutes. --keep a tab open to this link.




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



# 15. Plot explanation

There are 2 main LINE plots:  The ping delays of a close router [pingresult], and the TCP delays of top 100 web sites [Timetcpping].  These are the two colored lines.  The near ICMP ping delays and the TCP delays are every minute for 23 hours [2AM till next 1AM].  Typically, the near 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.

If "customerpings" are enabled, there will be a third line plot.

The third and fourth plot is the points that represent the twice hourly fetch of www.google.com - the curl time and the dns query time.  This will typically have the longest delay.  DNS name resolution will have to be performed for this, and for the TCP delays.  The ICMP ping delays do do a DNS name resolution.

The fifth and sixth "plot" is actually an overlay on the plots which will represent offline times experienced, and TCP timeouts experienced, 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.

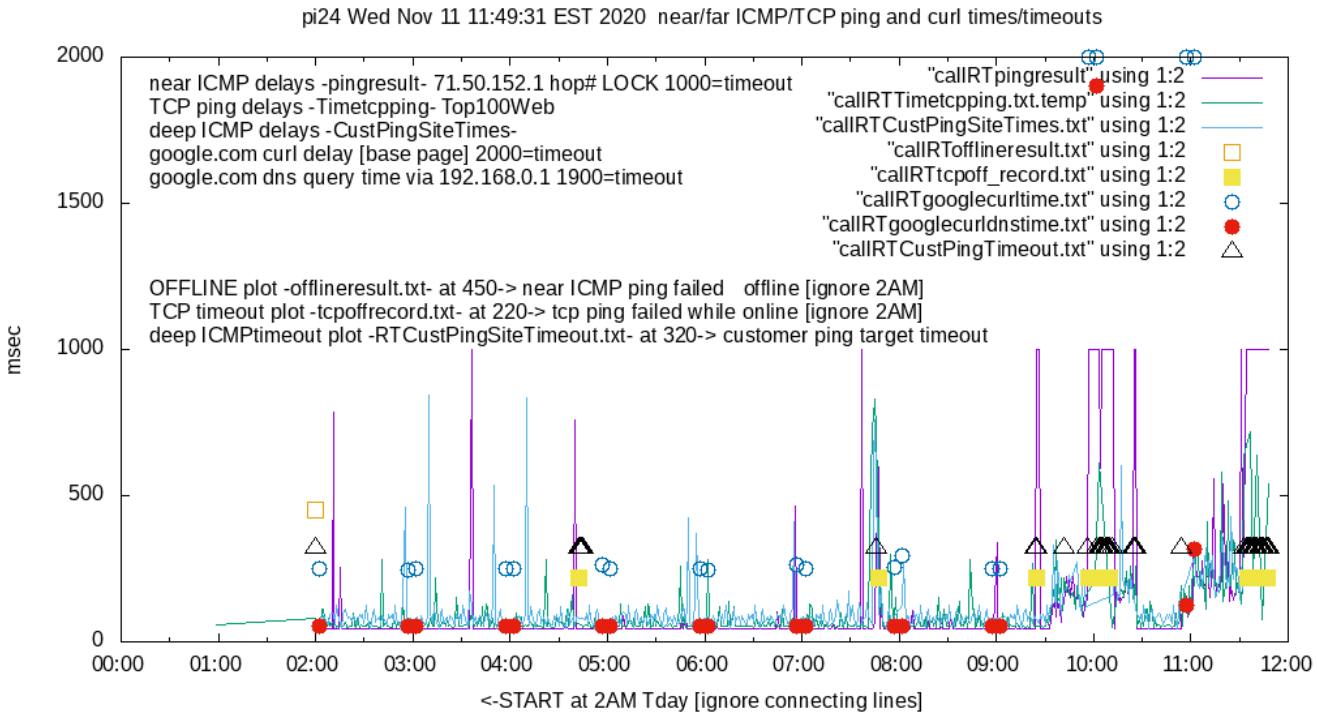
Added in Aug 2021 is the "hyperping" plot points.  This will be successive **vertical** ticks on the ICMP ping plot timeout line, which designate ping timeouts at 6/min rate, invoked when the 1/min ping rate fails.

As an option on the imonitorg, the customer can place a file "CustPingSites.newtxt" in the directory /home/pi/tests/customerpings/ and the scripts will automatically take up this file at [the next] 2AM and perform "deep ICMP" ping plotting.  Originally these sites represented the ping targets of imonitor [as opposed to imonitorg] customers, so they represented ICMP pingable sites 5- hops from each of the customers on the trial project across the US.  This file "CustPingSites.txt" was collected each night and copied to each pi for the use  of the "deep ICMP" plots the next day.  For the vbox imonitorg of course there is no connection to the main imonitorg server, so this file has to be manually constructed.  There is an example in the "files" of the sourceforge site https://imonitorg.sourceforge.io -the user can copy this file and use it, or modify it and place it in the customerpings directory.  This will only perform the pings for a 23 hour period starting at 2AM.  If the customer wants to make this plotting "permanent," he needs to make a pi crontab entry to replace his file in that directory each day.

E.g. save the file as CustPingSites.mytxt in /home/pi.  Make a pi crontab entry to cp the file to "CustPingSites.newtxt" each day anytime before 12AM.

25 23 * * * /bin/cp CustPingSites.mytxt tests/customerpings/CustPingSites.newtxt

This will copy the customer file to the directory each day at 11:25PM.  The CustPingsiteScript will use this script for the next day starting at 2AM.  Here is a [partial day using "create RTplot" on web page] sample plot showing the "deep ICMP" plotting:


pi24 Wed Nov 11 11:49:31 EST 2020 near/far ICMP/TCP ping and curl times/timeouts
near ICMP delays -pingresult- 71.50.152.1 hop# LOCK 1000=timeout
TCP ping delays -Timetcpping- Top100Web
deep ICMP delays -CustPingSiteTimes-
google.com curl delay [base page] 2000=timeout
google.com dns query time via 192.168.0.1 1900=timeout
"callRTpingresult" using 1:2
"callRTTimetcpping.txt.temp" using 1:2
"callRTCustPingSiteTimes.txt" using 1:2
"callRTofflineresult.txt" using 1:2
"callRTtcpoff_record.txt" using 1:2
"callRTgooglecurltime.txt" using 1:2
"callRTgooglecurldnstime.txt" using 1:2
"callRTCustPingTimeout.txt" using 1:2
OFFLINE plot -offlineresult.txt- at 450-> near ICMP ping failed offline [ignore 2AM]
TCP timeout plot -tcpoffrecord.txt- at 220-> tcp ping failed while online [ignore 2AM]
deep ICMPtimeout plot -RTCustPingSiteTimeout.txt- at 320-> customer ping target timeout
msec
2000
1500
1000
500
0
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
<-START at 2AM Tday [ignore connecting lines]