Gmail

John Loop <pccitizen@gmail.com>

John Loop's 4-23-2023 imonitorg newsletter: VMs, CGNAT, continuing work

1 message

John Loop <jdloop@imonitorg.com> Sun, Apr 23, 2023 at 11:10 AM
To: "pccitizen@gmail.com" <pccitizen@gmail.com>

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

Apologies if you do not want to receive this newsletter, sent 3,4 times per year [just reply to remove your email]. I have collected email addresses from some of my friends in hopes you might be interested.

*Summary for those of you new to this newsletter:**

I am working on a project to perform Internet/Local Network monitoring. I use a small device[raspberry pi3B or pi3B+], along with custom scripts to perform this service. I have deployed this device to 25+ partners across the country representing many different access technologies and ISPswho help in the development. I initially targeted the service in 2018 to assist in troubleshooting for my friends on our mountain, but it is applicable universally, and I have helpers across the country on Windstream, ATT, Ting, Spectrum, Comcast, CenturyLink, Tmobile, Starlink and several other ISPs. It spans all access technologies from ADSL, VDSL, WADSL, cellular, cable, satellite and fiber. I also created a "generic" version which is completely standalone, and has no connection to my servers at all. I posted these generic images on sourceforge.net. I also established a github page pointing to it. There is absolutely no third party server in the internet which you have to access to collect your info --it is all on a webpage on your local raspberry pi! All you have to do is download an image for a microSD card [you can get it from me if you want], plug it into your raspberry pi3B or 3B+, connect the ethernet and enjoy. You can configure an email using your gmail account as a relay. Instructions start here:

This month I am adding to this capability by providing VM [virtual machine] "ova" images so that you do not need a separate raspberry pi to perform this function. ...read on https://imonitorg.com

5-1-2023 newsletter

1. I have been working on creating a VM [virtual machine] image of the imonitorg function. This would be ideal for PCs or servers which are running 24/7 -you would not need a separate raspberry pi 3b or 3b+ device to perform the monitorg function! I have transferred the imonitor[g] scripts from the raspberry pi to an ubuntu OS [LTS 22.04] running in a VM. I then create an image of that VM - an "open virtual machine architecture [ova]" image which should be importable by VM hypervisors such as Oracle "VirtualBox," vmware "VMware," linux "boxes," Apple "parallels," and windows "Hyper-V." There are undoubtedly other hypervisors. I have tested the VM "ova" using Oracle "VirtualBox" on windows 10, rocky8 linux, and centos8 linux.

I am looking forward to testing the "ova" on other hypervisors, specifically vmware[runs on MACos], linux "boxes," and windows "hyper-V" in the coming months. "Parallels" is the MACos hypervisor, but they charge money, so I will probably not be testing this. I have a MAC M1 that I hope to install vmware on and test this. I would love any feedback, beta testers on this.

If you are not familiar with hypervisors, they are a very convenient way to run windows on your MAC, or linux on your windows, or windows on your linux, etc. etc. You just need the base "hypervisor" installed to manage it [plus the "virtualization" enable in the BIOS]. The hypervisor typically will list OS images [VMs in "ova" format] to import, or you can import your own, as we are doing here. The VM is bridged to the host network, to appear as just another PC/device on your network. It is a wonderful way to utilize multiple OS's, and is really superior to "dual boot" and similar techniques. Perhaps you have applications that only run on windows, but you are a "MAC" person. Just install "Parallels" and import the windows VM.

Most imonitor[g] scripts are transferred to the VM, including pihole. Since the VM appears "virtually" on the host network, it appears behind the network adapter of the host, which can be ethernet or wifi. So "wifi or "ethernet" is transparent to the VM. The wifi testing/scanning scripts are thus removed.

The first VM ova "vbox_imonitorg9.ova" is available at my sourceforge project page https://sourceforge.net/projects/imonitorg/files/

2. Tom -pi29- and I have been learning about "Carrier grade NAT [CGNAT]." Several ISPs implement their Internet access in this way. It has become increasingly apparent that this does not provide an "ID" on the Internet in the same manner as other ISPs -where "sticky" or "permanent" IP addresses are almost like real street addresses. pi29's "Internet IP" can change multiple times per hour at times. The CGNAT ISP manages the dance of the IP addresses so it can maintain TCP/UDP connectivity, much like cell phones can roam and stay connected. A CGNAT will thus not give you a "presence" on the Internet in the "traditional" way. You cannot run a service on a CGNAT connection, and associate a DNS domain to it. There are ways around this using VPNs and cloud servers of course. I will have to modify my script for CGNAT, because "your IP" on the Internet just doesn't really exist. The technology "TCP handoff" to manage this "dance" was invented for cellular phones that were IP.

I have "customers" like pi13 who have had the same Internet IP for 5 years. My Internet IP has not changed in 3 years -it only seems to change when huge storms rumble thru and send all of the local Spectrum network into a reboot. I would not doubt that this will likely change... no reason they can't save the IP to be sticky. There are many reasons why ISPs like your IP to be "sticky," not the least of course is that you can be ID'd by your IP, and this info can be sold. This is less and less useful with default DNS over https used in browsers [DOH]. In the old days you just rebooted you router to change your IP, but those days seem to be gone.

"StarLink" officially uses CGNAT, but the address change is far less often, at least in the case of pi8 and [former] pi9. You can even pay

more money and get a "real" ipv4 address. It is not quite clear why Starlink even does CGNAT, since it is only really used on ipv4 networks to preserve ipv4 address space. Starlink fully supports ipv6, so I suspect it is a transition issue. If a device has an ipv6 address, there is no reason to perform NAT of any type. .....of course there are legacy apps which only do ipv4, so the need for ipv4 will probably never go away.

Cellular networks, such as pi9 and pi14 also use CGNAT and most do ipv6, so there can be very confusing issues in trying to understand what they are doing. Ernie on pi9 [ATT firstnet] has only changed IP addresses once in a month since he has been on ATT firstnet. Matt on pi14 [ATT cellular broadband] has also not changed IP addresses.

In short if you are on a CGNAT-ISP network or a mobile network, you really do not have an "address" on the Internet similar to if you have a cable/fiber/ADSL -wired- access.

3. Cellular Broadband: "Cellular broadband" is appearing more and more. Tmobile may have been the first - Niel pi24 outside Raleigh NC used this for a year. It resembles voice cellular in its delay and congestion as can be seen by the response graphs. Spectrum provides this almost as a backup service now. I have it on a tablet in addition to regular Spectrum cable -this is undoubtedly Verizon broadband, since Spectrum uses Verizon here in FL. Ernie pi9 switched from Starlink to ATT firstnet, which is a cellular broadband. Matt -pi14 is testing ATT cellular broadband in N GA.

The performance of cellular broadband on these subs is a very good alternative to ADSL, and even the lower echelons of cable speed. It now offers unlimited data and download speeds maybe 50Mbs down. The only negatives are the congestion and delay experienced, since they are in effect competing for voice on the physical airwaves. And of course remember, these technologies are all "in the air" like wifi, so they are not secure like fiber or wires.

The other "air-only" access pis are Tom's WADSL pi29 and 31 in N CO. WADSL is like ADSL except over the air using line of site transmitters/receivers -Tom has an antenna pointed at the server! Performance specs are similar to ADSL. The unique aspect of Tom's pi29 is the CGNAT provisioning.

4. Fiber access: It is amazing how fiber access is accelerating. I can remember working on fiber broadband sysems at Bellcore where this was a dream. This was in 1986 or so. On our imonitor trial, pi22, 23, 24, 27 and 32 are fiber connections now [ATT, Ting, Longmont, Estes Park]. The performance of these access technologies is amazing -just look at their performance plots. https://imonitorg.com/customerplots/rtcustomerplots -click on the first link up there. Access speed is "normally" about 1Gbs downspeed, and is very hard to "measure."

5. Cable access: pi11 is cable access technologies with lower performance [lower cost]. pi 1,3,6.5,10,15,20,21,25,26,16 are higher peformance cable [Comcast, Spectrum, TDS], often approaching 1Gbs downspeed. I remember the telco [ADSL] guy fearing cable would overtake them, and it pretty much has! Centurylink, which is mostly telco wires, is still around as a second choice in many of these areas [like mine].

6. ADSL access: Phil on pi7,12 and 13 and Kevin on pi28 are the last "pioneers" using the phone line pair -ADSL -mostly VDSL technologies. It is amazing that we lived -almost- thru the demise of the phone line pair as an access technology. It was such a truly marvelous step forward when simple ADSL came out about 1995 with 1.5Mbs down, shared with your voice line. Almost 30 years ago!

7. Speedtests: it is increasingly misleading to measure the speed of these connections. It depends so much on the client and the network the ISP puts in place to measure your speed. Just how do you measure speed on a statisically multiplexed connection? If two packets are back to back in the medium, do you declare the speed as "line speed." There are so many algorithms for doing this that it is another study. I like to use "Speed.cloudflare.com" which shows a time graph of your speed. I am sure the speed it "reports" is probably the PEAK it sees.

8. IPv6: Routers allow outgoing IPv6 [and the corresponding return packets], but defaultly block unsolicited incoming IPv6 TCP connections. There are very few routers which allow mapping ports on IPv6 addresses. And don't dare do a DNS entry for your ipv6 address if you can't forward the port. ...you can do all this using ipv4 almost universally. Very confusing to sort out the alternatives!!

I am doing inventory on my pis WRT ipv6 and making sure I understand the situation where it is provided/not provided and when it is disabled/not provided. Several pis appear as a second stage NAT on the home network, and the second stage router is not doing ipv6 passthru so the pi can see the ipv6. Several people have ipv6 turned off, tho this should not be necessary. Almost all applications these days, such as thunderbird and your browser will try ipv6 connections first if they get ipv6 addresses for names. This should "always" work, but if you get delays initially, it is because the ipv6 is timing out [several minutes worth] and will eventually flip to ipv4. I am troubleshooting a problem on my thunderbird where this happens, tho ipv6 is functioning on my connection. Go to "testipv6.com" in a browser, e.g. to get a report on your ipv6 capabilty.

9. I recently added a script to the pis to monitor for "off-network" unsolicited TCP connections to the pi. These should never happen unless you have a port mapped to the pi in your router. They will be triggered e.g. if you switch networks in your home and the pi has not adjusted to the new IP, so it should be transitory.

This is a link to the imonitorg.com homepage, which has a listing of all previous newsletters. https://imonitorg.com

I ardently hope for corrections and discussions of any of the topics above. Thank you.

John Loop 4-20-2023

--