Network Traffic Monitor Monthly Report

Generated on 2024-07-01

Device Info:

Host Name:	DESKTOP-C8GFQ4G
OS Name:	Microsoft Windows 10 Pro
OS Version:	10.0.19045 N/A Build 19045
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
Registered Owner:	N/A
Registered Organization:	N/A
Product ID:	00331-20350-38045-AA829
Original Install Date:	4/5/2023, 3:13:17 AM
System Boot Time:	30/6/2024, 5:36:36 PM
System Manufacturer:	Gigabyte Technology Co., Ltd.
System Model:	H410M S2 V2
System Type:	x64-based PC
Processor(s):	1 Processor(s) Installed.
	[01]: Intel64 Family 6 Model 165 Stepping 5 GenuineIntel ~2904 Mhz
BIOS Version:	American Megatrends Inc. F1, 20/1/2021
Windows Directory:	C:\WINDOWS
System Directory:	C:\WINDOWS\system32
Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)
Input Locale:	en-us;English (United States)
Time Zone:	(UTC+08:00) Kuala Lumpur, Singapore
Total Physical Memory:	32,681 MB
Available Physical Memory:	18,085 MB
Virtual Memory: Max Size:	37,545 MB
Virtual Memory: Available:	15,477 MB
Virtual Memory: In Use:	22,068 MB
Page File Location(s):	C:\pagefile.sys
Domain:	WORKGROUP
Logon Server:	\\DESKTOP-C8GFQ4G

Network IP Info:

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C8GFQ4G
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (11) I219-V
   Physical Address. . . . . . . . . : 18-C0-4D-BE-A8-D8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::93b2:8c69:159f:3325%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.34(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, 30 June, 2024 5:37:10 PM
   Lease Expires . . . . . . . . . . : Tuesday, 2 July, 2024 5:37:07 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 102285389
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-E4-67-13-18-C0-4D-BE-A8-D8
   DNS Servers . . . . . . . . . . . : fe80::6ba:d6ff:fe5f:9870%11
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c03a:1044:759:f663%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 688521255
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-E4-67-13-18-C0-4D-BE-A8-D8
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8723B Wireless LAN 802.11n USB 2.0 Network Adap
   Physical Address. . . . . . . . . : 00-13-EF-1F-00-D6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 02-13-EF-1F-00-D6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

```
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 00-13-EF-1F-00-D6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter ZeroTier One [af78bf94362c96df]:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : ZeroTier Virtual Port
   Physical Address. . . . . . . . . : DE-45-5C-F3-CA-BF
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6e34:1d42:6188:7f2e%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.22.176.83(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 25.255.255.254
   DHCPv6 IAID . . . . . . . . . . . : 987645276
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-E4-67-13-18-C0-4D-BE-A8-D8
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 00-13-EF-1F-00-D6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Ping Sweep Logs:

ID	Timestamp	Start IP	End_IP
1	2024-07-01 08:19:35	192.168.0.0	192.168.0.4
2	2024-07-01 08:42:49	192.168.56.0	192.168.56.5
3	2024-07-01 08:42:53	169.254.0.0	169.254.255.255
4	2024-07-01 08:42:56	169.254.0.0	169.254.255.255
5	2024-07-01 08:42:58	172.22.0.0	172.22.255.255

IP Traffic Detected On Network:

192.168.0.34 (DESKTOP-C8GFQ4G)

- 192.168.0.34 (186.152.213.35.bc.googleusercontent.com)
- 192.168.0.34 (101.182.213.35.bc.googleusercontent.com)
- 192.168.0.34 (Hostname N/A)
- 192.168.0.34 (192.168.0.1)
- 192.168.0.34 (root-sgp-01.zerotier.com)
- 192.168.0.34 (78.184.209.35.bc.googleusercontent.com)
- 192.168.0.34 (edge-dgw-shv-02-kul2.facebook.com)
- 192.168.0.34 (edge-dgw-shv-01-kul2.facebook.com)
- 192.168.0.34 (139.179.213.35.bc.googleusercontent.com)
- 192.168.0.34 (anonymous)
- 192.168.0.34 (227.211.149.34.bc.googleusercontent.com)
- 192.168.0.34 (instagram-p3-shv-02-kul2.fbcdn.net)
- 192.168.0.34 (ec2-50-19-50-5.compute-1.amazonaws.com)
- 192.168.0.34 (ec2-54-151-156-30.ap-southeast-1.compute.amazonaws.com)
- 192.168.0.34 (bt1.us.archive.org)
- 192.168.0.34 (ec2-44-223-254-189.compute-1.amazonaws.com)
- 192.168.0.34 (ec2-54-227-133-51.compute-1.amazonaws.com)
- 192.168.0.34 (edge-star-mini-shv-01-kul2.facebook.com)
- 192.168.0.34 (root-zrh-01.zerotier.com)
- 192.168.0.34 (ec2-3-209-49-252.compute-1.amazonaws.com)
- 192.168.0.34 (103-10-124-124.valve.net)
- 192.168.0.34 (222-169.175.103.static.gtplkcbpl.in)
- 192.168.0.34 (109-252-106-114.nat.spd-mgts.ru)
- 192.168.0.34 (whatsapp-cdn-shv-02-kul2.fbcdn.net)
- 192.168.0.34 (vmi676926.contaboserver.net)
- 192.168.0.34 (pool-72-69-82-190.nycmny.fios.verizon.net)
- 192.168.0.34 (109.122.98.34.bc.googleusercontent.com)
- 192.168.0.34 (253.85.120.34.bc.googleusercontent.com)
- 192.168.0.34 (192.168.0.17)
- 192.168.0.34 (root-mia-01.zerotier.com)
- 192.168.0.34 (sf-in-f188.1e100.net)
- 192.168.0.34 (kul06s11-in-f35.1e100.net)
- 192.168.0.34 (igmp.mcast.net)
- 192.168.0.34 (ward-12-b2-v4wan-170702-cust517.vm18.cable.virginm.net)
- 192.168.0.34 (net176113006017.pskovline.ru)
- 192.168.0.34 (shiva.theonlyhost.co.uk)
- 192.168.0.34 (191-194-160-187.user.vivozap.com.br)
- 192.168.0.34 (hn.kd.ny.adsl)
- 192.168.0.34 (ppp046103061141.access.hol.gr)

35.213.179.139 (139.179.213.35.bc.googleusercontent.com)

- 35.213.179.139 (DESKTOP-C8GFQ4G)

35.213.182.101 (101.182.213.35.bc.googleusercontent.com)

- 35.213.182.101 (DESKTOP-C8GFQ4G)

35.213.152.186 (186.152.213.35.bc.googleusercontent.com)

- 35.213.152.186 (DESKTOP-C8GFQ4G)

162.159.137.232 (Hostname N/A)

- 162.159.137.232 (DESKTOP-C8GFQ4G)

175.11.240.224 (Hostname N/A)

- 175.11.240.224 (DESKTOP-C8GFQ4G)

35.209.184.78 (78.184.209.35.bc.googleusercontent.com)

- 35.209.184.78 (DESKTOP-C8GFQ4G)

163.70.137.8 (edge-dgw-shv-02-kul2.facebook.com)

- 163.70.137.8 (DESKTOP-C8GFQ4G)

163.70.132.10 (edge-dgw-shv-01-kul2.facebook.com)

- 163.70.132.10 (DESKTOP-C8GFQ4G)

162.159.138.234 (Hostname N/A)

- 162.159.138.234 (DESKTOP-C8GFQ4G)

192.168.0.4 (anonymous)

- 192.168.0.4 (DESKTOP-C8GFQ4G)
- 192.168.0.4 (igmp.mcast.net)

34.149.211.227 (227.211.149.34.bc.googleusercontent.com)

- 34.149.211.227 (DESKTOP-C8GFQ4G)

162.159.128.235 (Hostname N/A)

- 162.159.128.235 (DESKTOP-C8GFQ4G)

163.70.137.63 (instagram-p3-shv-02-kul2.fbcdn.net)

- 163.70.137.63 (DESKTOP-C8GFQ4G)

162.159.129.235 (Hostname N/A)

- 162.159.129.235 (DESKTOP-C8GFQ4G)

192.168.0.17 (anonymous)

- 192.168.0.17 (DESKTOP-C8GFQ4G)
- 192.168.0.17 (igmp.mcast.net)
- 192.168.0.17 (mdns.mcast.net)

104.18.137.67 (Hostname N/A)

- 104.18.137.67 (DESKTOP-C8GFQ4G)

104.26.6.202 (Hostname N/A)

- 104.26.6.202 (DESKTOP-C8GFQ4G)

54.151.156.30 (ec2-54-151-156-30.ap-southeast-1.compute.amazonaws.com)

- 54.151.156.30 (DESKTOP-C8GFQ4G)

162.159.133.234 (Hostname N/A)

- 162.159.133.234 (DESKTOP-C8GFQ4G)

192.168.0.8 (c6n_bb2199857_ezviz)

- 192.168.0.8 (Hostname N/A)

116.74.59.105 (Hostname N/A)

- 116.74.59.105 (DESKTOP-C8GFQ4G)

192.168.0.3 (d76270767)

- 192.168.0.3 (igmp.mcast.net)

20.198.119.84 (Hostname N/A)

- 20.198.119.84 (DESKTOP-C8GFQ4G)

44.223.254.189 (ec2-44-223-254-189.compute-1.amazonaws.com)

- 44.223.254.189 (DESKTOP-C8GFQ4G)

117.18.232.200 (Hostname N/A)

- 117.18.232.200 (DESKTOP-C8GFQ4G)

54.227.133.51 (ec2-54-227-133-51.compute-1.amazonaws.com)
- 54.227.133.51 (DESKTOP-C8GFQ4G)

163.70.132.35 (edge-star-mini-shv-01-kul2.facebook.com)
- 163.70.132.35 (DESKTOP-C8GFQ4G)

52.123.172.10 (Hostname N/A)
- 52.123.172.10 (DESKTOP-C8GFQ4G)

217.156.67.96 (Hostname N/A)
- 217.156.67.96 (DESKTOP-C8GFQ4G)

104.208.16.91 (Hostname N/A)
- 104.208.16.91 (DESKTOP-C8GFQ4G)

3.209.49.252 (ec2-3-209-49-252.compute-1.amazonaws.com)
- 3.209.49.252 (DESKTOP-C8GFQ4G)

103.10.124.124 (103-10-124-124.valve.net)
- 103.10.124.124 (DESKTOP-C8GFQ4G)

46.232.211.180 (Hostname N/A)
- 46.232.211.180 (DESKTOP-C8GFQ4G)

103.175.169.222 (222-169.175.103.static.gtplkcbpl.in)
- 103.175.169.222 (DESKTOP-C8GFQ4G)

163.70.137.60 (whatsapp-cdn-shv-02-kul2.fbcdn.net)
- 163.70.137.60 (DESKTOP-C8GFQ4G)

104.46.162.227 (Hostname N/A)
- 104.46.162.227 (DESKTOP-C8GFQ4G)

220.94.193.80 (Hostname N/A)

- 220.94.193.80 (DESKTOP-C8GFQ4G)

192.168.0.1 (192.168.0.1)

- 192.168.0.1 (DESKTOP-C8GFQ4G)

66.94.102.63 (vmi676926.contaboserver.net)

- 66.94.102.63 (DESKTOP-C8GFQ4G)

204.79.197.239 (Hostname N/A)

- 204.79.197.239 (DESKTOP-C8GFQ4G)

202.188.238.210 (Hostname N/A)

- 202.188.238.210 (DESKTOP-C8GFQ4G)

202.188.238.218 (Hostname N/A)

- 202.188.238.218 (DESKTOP-C8GFQ4G)

72.69.82.190 (pool-72-69-82-190.nycmny.fios.verizon.net)

- 72.69.82.190 (DESKTOP-C8GFQ4G)

34.98.122.109 (109.122.98.34.bc.googleusercontent.com)

- 34.98.122.109 (DESKTOP-C8GFQ4G)

46.232.211.160 (Hostname N/A)

- 46.232.211.160 (DESKTOP-C8GFQ4G)

192.168.0.17 (192.168.0.17)

- 192.168.0.17 (DESKTOP-C8GFQ4G)

74.125.24.188 (sf-in-f188.1e100.net)

- 74.125.24.188 (DESKTOP-C8GFQ4G)

192.168.0.16 (esp_a92c8e)

- 192.168.0.16 (mdns.mcast.net)

85.248.73.195 (Hostname N/A)

- 85.248.73.195 (DESKTOP-C8GFQ4G)

103.199.144.42 (ns2.blss.in.144.199.103.in-addr.arpa)

- 103.199.144.42 (DESKTOP-C8GFQ4G)

192.168.0.13 (d18473575)

- 192.168.0.13 (igmp.mcast.net)

86.21.194.6 (ward-12-b2-v4wan-170702-cust517.vm18.cable.virginm.net)

- 86.21.194.6 (DESKTOP-C8GFQ4G)

192.168.0.6 (anonymous)

- 192.168.0.6 (Hostname N/A)
- 192.168.0.6 (mdns.mcast.net)

10.248.203.7 (10.248.203.7)

- 10.248.203.7 (all-systems.mcast.net)

192.168.0.21 (c6n_bb2199819_ezviz)

- 192.168.0.21 (Hostname N/A)

46.232.211.231 (Hostname N/A)

- 46.232.211.231 (DESKTOP-C8GFQ4G)

51.89.235.77 (shiva.theonlyhost.co.uk)

- 51.89.235.77 (DESKTOP-C8GFQ4G)

52.123.168.218 (Hostname N/A)

- 52.123.168.218 (DESKTOP-C8GFQ4G)

190.83.252.80 (Hostname N/A)

- 190.83.252.80 (DESKTOP-C8GFQ4G)

178.162.173.198 (Hostname N/A)

- 178.162.173.198 (DESKTOP-C8GFQ4G)

111.38.106.19 (Hostname N/A)

- 111.38.106.19 (DESKTOP-C8GFQ4G)

191.194.160.187 (191-194-160-187.user.vivozap.com.br)

- 191.194.160.187 (DESKTOP-C8GFQ4G)

50.19.50.5 (ec2-50-19-50-5.compute-1.amazonaws.com)

- 50.19.50.5 (DESKTOP-C8GFQ4G)

192.168.0.37 (noels-galaxy-note9)

- 192.168.0.37 (mdns.mcast.net)

NMAP Scan Logs:

ID	Timestamp	Scan	IP	Start Port	End Port
1	2024-07-01 11:56:18	TCP Connect Scan	192.168.0.34	1	10
2	2024-07-01 11:56:31	SYN Scan	192.168.0.34	1	10
3	2024-07-01 11:56:38	OS Detection	192.168.0.34	1	10
4	2024-07-01 11:56:51	List Scan	192.168.0.34	1	10
5	2024-07-01 11:57:08	Aggressive Scan	192.168.0.34	1	10
6	2024-07-01 11:57:17	Ping Scan	192.168.0.34	1	10

Traffic Volume by IP Src to IP Dest:

IP_Src	IP_Dest	Average	Count	Alerts	Total

High Traffic Alerts:

Timestamp	IP_Src	IP_Dest	Average	Threshold	Count
2024-07-01 12:29:09	35.213.152.186	192.168.0.34	7.71	50	118.0
2024-07-01 12:29:10	192.168.0.34	35.213.152.186	194.14	50	531.0
2024-07-01 12:29:10	35.213.179.139	192.168.0.34	15.0	50	194.0
2024-07-01 12:29:32	192.168.0.34	35.213.152.186	247.67	50	1270.0
2024-07-01 12:29:32	35.213.179.139	192.168.0.34	34.38	50	202.0
2024-07-01 12:29:33	192.168.0.34	35.213.179.139	1.33	50	103.0
2024-07-01 12:29:33	35.213.152.186	192.168.0.34	16.0	50	116.0

Suspicious Packet Alerts:

Timestamp	File	Type
2024-07-01 04:57:34	2024-07-01 04-57-34_87e904d9-781d-4461-a3f0-1a867a228470.pcap	Test Fault