# Anonymizing your MAC address

configuration, version-r41, security, networking

taradiddles 1 June 3, 2023, 12:59pm

Although the MAC address is not the only metadata broadcast by network hardware, changing your hardware's default MAC Address could be an important step in protecting privacy.

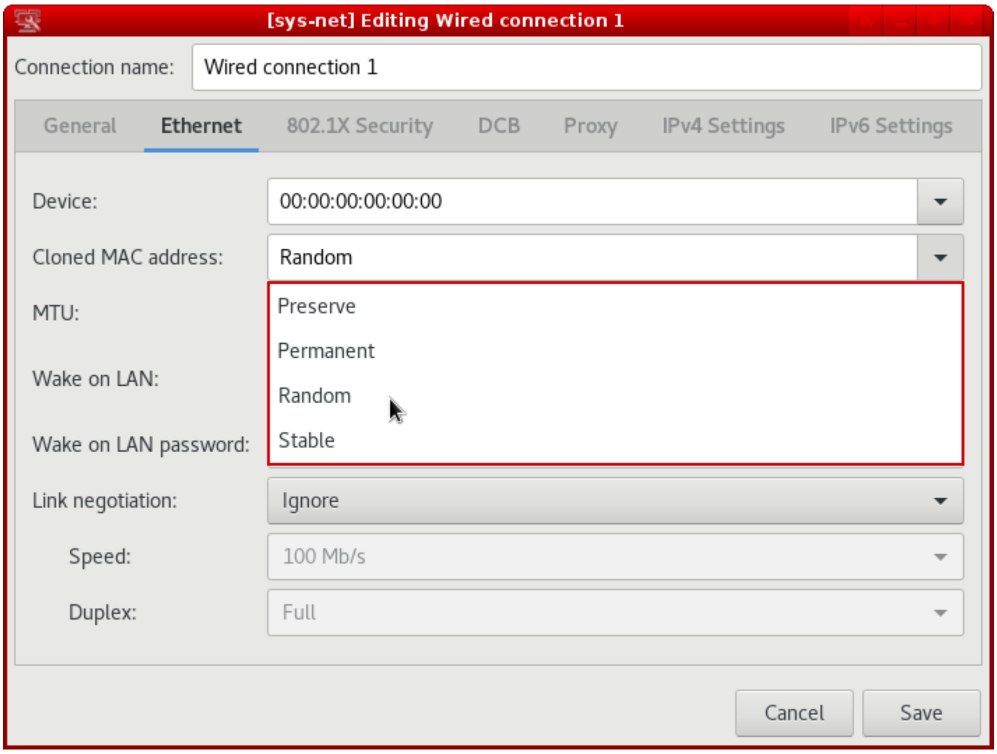
Qubes OS 4.1 and later already anonymize all Wi-Fi MAC addresses by default - they change during every Wifi session. So there is **no need** to apply any of the instructions below if you're only interested in Wi-Fi connections. Users requiring Ethernet MAC address anonymization may want to read on.

# Randomize a single connection

Right click on the Network Manager icon of your NetVM in the tray and click 'Edit Connections…'.

Select the connection to randomize and click Edit.

Select the "Cloned MAC Address" drop-down list and pick either 'Random" or "Stable'. 'Stable' will generate a random address that persists until reboot, while 'Random' will generate an address each time a link goes up.



[sys-net] Editing Wired connection 1

Connection name: Wired connection 1

Device: 00:00:00:00:00:00

Cloned MAC address: Random

MTU:

Wake on LAN:

Wake on LAN password:

Link negotiation: Ignore

Speed: 100 Mb/s

Duplex: Full

Save the change and reconnect the connection (click on Network Manager tray icon and click "Disconnect" under the connection, it should automatically reconnect).

# Randomize all Ethernet and Wi-Fi connections

These steps should be done inside the template of the NetVM to change as it relies on creating a config file that would otherwise be deleted after a reboot due to the nature of AppVMs.

Write the settings to a new file in the `/etc/NetworkManager/conf.d/` directory, such as `50-macrandomize.conf`. The following example enables Wi-Fi and Ethernet MAC address randomization while scanning (not connected), and uses a randomly generated but persistent MAC address for each individual Wi-Fi and Ethernet connection profile. It was inspired by the **official NetworkManager example**.

```
[device]
wifi.scan-rand-mac-address=yes

[connection]
wifi.cloned-mac-address=stable
ethernet.cloned-mac-address=stable
connection.stable-id=${CONNECTION}/${BOOT}
ipv6.dhcp-duid=stable-uuid

#the below settings is optional (see the explanations below)
ipv6.ip6-privacy=2
```

- `cloned-mac-address=stable` in combination with `connection.stable-id=${CONNECTION}/${BOOT}` generates a random MAC address that persists until reboot. You could use `connection.stable-id=random` instead, which generates a random MAC address each time a link goes up.
- `ipv6.dhcp-duid=stable-uuid` will prevent that the DHCP client identifier in IPv6 is looked up from a global lease file. The current default behaviour for IPv4 is to use the already random MAC as DHCP client identifier.
- `ipv6.ip6-privacy=2` will cause multiple random IPv6 addresses to be used during every session (cf. **RFC 4941**). If you want to use a fixed IPv6 address based on the already random MAC address, choose `ipv6.ip6-privacy=0`. Leaving this setting at the default is not recommended as it is basically undefined.

Also make sure that you have `addr-gen-mode=stable-privacy` in the `[ipv6]` section of your `/rw/config/NM-system-connections/*.nmconnection` files as this setting can only be set per connection.

To see all the available configuration options, refer to the man page: `man nm-settings`

You can check the MAC address currently in use by looking at the status pages of your router device(s), or inside the NetVM with the command `sudo ip link show`.

# Anonymize your hostname

DHCP requests *may* also leak your hostname to your LAN. Since your hostname is usually `sys-net`, other network users can easily spot that you're using Qubes OS.

Unfortunately `NetworkManager` currently doesn't provide an option to disable that leak globally (**NetworkManager bug 584**).

However the `NetworkManager` versions as of Qubes OS 4.1 were found to not leak the hostname as long as the file `/etc/hostname` does **not** exist. This behaviour may be subject to change in future `NetworkManager` versions though. So please always double check whether your hostname is leaked or not on e.g. your home router, via `wireshark` or `tcpdump`.

If you want to decide per connection, `NetworkManager` provides an option to not send the hostname:
Edit the saved connection files at `/rw/config/NM-system-connections/*.nmconnection` and add the `dhcp-send-hostname=false` line to both the `[ipv4]` and the `[ipv6]` section.

► This document was migrated from the qubes-community project
2 Likes

Mac Address tweak no longer apply in 4.2?

Qubes OS privacy enhancement guide

Qubes need CCcleaner thing and macannony thig?

Troubleshooting solution for minimal VPN qube(s) on 4.2

Iptables not available in sys-net in Qubes OS 4.2.1

Mac randomization not working

Where to learn more about security implementations in QubesOS

Qubes Inplace upgrade from 4.1-4.2 issues

No20 2 November 19, 2023, 8:23pm

Very good guide!

One little addition:

IMHO if `ipv6.ip6-privacy=0` is set, the IPv6 address is not based on the already random MAC address via the (modified) EUI-64 scheme but rather the stable private address scheme (RFC 7217) is used to created the IPv6 address since NetworkManager uses this as the default scheme (NetworkManager Docs IPv6).
This scheme uses the host specific key, the interface name, the connection's "connection.stable-id" property and the address prefix to create the random MAC (loc. cit.). Hence, at every Boot (as defined in the connection.stable-id property in your config) a new unqiue random IPv6 address is created via this scheme (NetworkManager Docs connection).
The difference is that the created IPv6 address does not include the randomly created MAC address as would be the case when using the EU-64 method.

Just saw this point and wanted to clarify it.

Best!

2 Likes

qubist 3 November 22, 2023, 10:43am

> **How to avoid exposing my MAC address when using IPv6?**
>
> ipv6, privacy, mac-address
>
> asked by Arjan on 05:26PM - 09 Feb 11 UTC

---

Zeno 4 February 11, 2024, 12:04pm

After creation of `50-macrandomize.conf` → shutting down the template → rebooting `sys-net`, I'm getting "NetworkManager is not running…` on the systray icon.

Removing/renaming the `50-macrandomize.conf` brings the connection back.

---

QUilleen 5 February 11, 2024, 11:19pm

AFAIK Qubes does this automatically on boot, right?

---

ava 6 June 16, 2024, 9:43pm

For WiFi yes MAC address anonymization, yes.

> Qubes OS 4.1 and later already anonymize all **Wi-Fi MAC** addresses by default - they change during every Wifi session. So there is **no need** to apply any of the instructions below if you're only interested in Wi-Fi connections.

> Users requiring **Ethernet MAC** address anonymization may want to read on.

So, if you require Ethernet MAC (as in, wired) address anonymization you may want to read on and/or apply the steps covered 🙂

---

sn00per 7 September 13, 2024, 7:47pm

> taradiddles:
>
> Qubes OS 4.1 and later already anonymize all Wi-Fi MAC addresses by default - they change during every WiFi session.

What happens if you additionally activate Cloned MAC Random or Stable in the NetworkManager Applet for a WiFi connection with regard to the MAC address configuration? Based on my test a WiFi connection did not work anymore but this could be due to a mistake of me.

Is the MAC randomization also established by default when attaching an external USB WiFi adapter?

As MAC randomization is not activated for Ethernet connections by default, what happens regarding MAC address configuration if you attach an external USB WiFi router (e.g. WiFi Pineapple) and activate Cloned MAC Random or Stable in the NetworkManager Applet for that recognized Ethernet connection? Because usually you change the MAC address for these devices on their administration user interface.

---

**ghostsinthebaseband** 8 September 13, 2024, 10:06pm

There are more intensive probing techniques that an adversary may use to profile and obstruct Qubes networking.

Macchiato is more sophisticated than the default MAC changer this guide discusses and it may be worth incorporating into your system.

Also ICMP echo responses and deep stack interrogation are utilized to target and disrupt Qubes systems.

What can you do about a psychopathic adversary like a hostile ISP and NSA? Not just the cops in skill but just as stupid, selfish, abusive, and unaccountable.

---

**apparatus** 9 September 16, 2024, 9:53am

> sn00per:
>
> What happens if you additionally activate Cloned MAC Random or Stable in the NetworkManager Applet for a WiFi connection with regard to the MAC address configuration? Based on my test a WiFi connection did not work anymore but this could be due to a mistake of me.

I think the configuration in NetworkManager Applet would take priority but I'm not sure so you should test it.

> sn00per:
>
> Is the MAC randomization also established by default when attaching an external USB WiFi adapter?

Yes.

> sn00per:
>
> As MAC randomization is not activated for Ethernet connections by default, what happens regarding MAC address configuration if you attach an external USB WiFi router (e.g. WiFi Pineapple) and activate Cloned MAC Random or Stable in the NetworkManager Applet for that

> recognized Ethernet connection? Because usually you change the MAC address for these devices on their administration user interface.

If USB WiFi router is trusted then I think there is a little value in randomizing the Ethernet MAC address because your PC Ethernet MAC address connected to USB WiFi router will only be seen by the USB WiFi router and won’t go outside it.
The MAC address is only seen for the devices in the same LAN.

1 Like