



# In the Boxing Ring October 2020



## Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

### Welcome to the October 2020 edition of In the Boxing Ring

This month, we are talking about **Privacy and MAC Address Randomization**. A MAC (Media Access Control) address is a network address assigned to a physical device. These are used on Ethernet ports, as well as WiFi and Bluetooth endpoints, to identify your devices uniquely. In their latest operating systems, both Google and Apple use randomized MAC addresses. On pages 2 to 3, we discuss what this is and why it was done, and highlight both its positive and negative impact.

On page 4, we highlight the features and fixes to be released in this quarter's Patch Tuesday for Network Box 5.

In other news, Network Box is excited to announce our latest revision to the **E-Series** hardware units. Additionally, Network Box Germany's Dariush Ansari, together with partner *IT-On.NET*, has launched an IT Security podcast title **HPCC Hackpod Club**. And in this month's Media Coverage, Network Box was featured in **Brilliance Security Magazine, EME Outlook, China Daily, and Banking Today**.



**Mark Webb-Johnson**  
CTO, Network Box Corporation Ltd.  
October 2020

### Stay Connected

You can contact us here at Network Box HQ by email: **[nbhq@network-box.com](mailto:nbhq@network-box.com)**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:



<https://twitter.com/networkbox>



<https://www.facebook.com/networkbox>  
<https://www.facebook.com/networkboxresponse>



<https://www.linkedin.com/company/network-box-corporation-limited/>



<https://www.youtube.com/user/NetworkBox>

### In this month's issue:

#### Page 2 to 3

#### Privacy and MAC Address Randomization

With the release of iOS 14, Apple follows Google's lead and turns on MAC address randomization by default. In our featured article, we discuss this, why it was done, and its possible impact.

#### Page 4

#### Network Box 5 Features

The features and fixes to be released in this quarter's Patch Tuesday for Network Box 5.

#### Page 5

#### Network Box Highlights:

- **Network Box Hardware Upgrades:**
  - S-80i
  - M-255i
  - E-Series
- **Network Box Media Coverage:**
  - Brilliance Security Magazine
  - EME Outlook
  - China Daily
  - Banking Today



# Privacy and MAC Address Randomization

**With the release of iOS 14, Apple follows Google's lead and turns on MAC address randomization by default. What is this? Why was it done? And what is the impact (both positive and negative)?**

## MAC Addresses used for Tracking

A MAC (Media Access Control) address is a network address assigned to a physical device. These are used on Ethernet ports, as well as WiFi and Bluetooth endpoints. They are 48 bits in length (6 bytes) and often written as six pairs of hexadecimal numbers (such as 00:0a:95:9d:68:16). The numbers themselves are administered by the IEEE (Institute of Electrical and Electronics Engineers) organizations. Typically, the first three bytes are used to identify the organization and the remaining three bytes, then sub-assigned by that organization to individual hardware components they manufacture. Every network device gets a unique MAC address for each networking technology/port.

As MAC addresses are used for physical addressing, they are most often sent unencrypted on the network, and are often used in protocol broadcast traffic (received by all nodes in the local network). It is trivial for any node on the network to listen for and collate the MAC addresses of all other nodes on the same network. The manufacturer can then be identified, and as each MAC address is uniquely assigned to one hardware device, that device can be tracked. In particular, the device could also be tracked as it passes between different networks.

Let's use, as an example, the WiFi protocol. As you walk in and out of shops around a mall, your phone is listening for WiFi networks and trying to connect. All this traffic involves MAC addresses, and it becomes possible to track you as you move between locations.



## Randomized MAC addresses

The issue here is the MAC address assigned to your phone's WiFi module or network card. As the MAC address is fixed, it becomes something that uniquely identifies you (or at least your phone).

In their latest operating systems, the workaround now implemented by both Google and Apple is to instead use randomized MAC addresses for each network being communicated with. Every time the phone tries to connect to the network, it uses a different randomly created MAC address - making it impossible (at least trivially) to track you. The identifier is no longer unique for any extended period of time or between different networks.

The advantage here is clear. The solution offers a degree of protection for your privacy, with associated improvements in your security.

## Why is this a problem?

There are several drawbacks to this approach, which we must be aware of. Here are a few of the most impacting:

- The DHCP protocol (Dynamic Host Configuration Protocol) is commonly used to assign IP addresses to connect workstations and phones, tablets, and other such devices. This assignment is based on the MAC address. It relies on the MAC address being associated with the hardware endpoint, to lease a stable IP address from a limited pool of available address space. The issue with MAC randomization is that the MAC address is no longer stable and cannot be reused quickly, which leads to wasted address allocations and exhaustion of the pool of available addresses. MAC address randomization increases the workload on DHCP and wastes addresses. Administrative changes will have to be made to either increase the pool's size or decrease lease allocation times to compensate.
- While IEEE assigned MAC addresses are guaranteed to be unique, randomized MAC addresses are not. It is possible for two devices to choose the same address independently randomly. Should that happen, they will interfere with each other and be unable to connect to the network or disconnect if already connected.
- Your company may need to track you. With the increase in the importance of approaches such as BYOD (Bring Your Own Device), or with static IP address allocations over DHCP, your phone's MAC address is necessary for your company to be able to handle your device correctly when it enters their network. Upgrade to iOS 14, and things may break.

**The solution to these issues is for IT staff to be aware of the technology and the possible impacts on the networks they manage. DHCP settings can be adjusted, and for those cases where a physical MAC address is required, the user instructed to turn off the 'private MAC address' (aka MAC address randomization) for that network.**

**MAC address randomization is a powerful feature offering improvements to both privacy and security. However, it is not without its drawbacks, particularly in corporate network environments.**

# Network Box



## NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th October 2020, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

## Network Box 5 Features October 2020

This quarter, for Network Box 5, these include:

- Increase of default memory allocated to stream processing on high end Network Box models, to increase throughput limits and performance
- Implement support for 'destination host' when using SSL/TLS proxy
- Improvements in application identification and promotion in protocols with early server responses
- Improvements to SSL/TLS proxy during protocol handshake with protocols driven from client side
- Introduce support to allow the generic proxy timeout to be configurable
- Improved support for cluster sync connections offering duplicate device IDs
- Improved support for QoS on generic UDP protocol proxy
- Add a VPN id filter to VPN / Event Logs report on admin web portal
- Improvements to VPN session summary on admin web portal
- Add 'entity' and 'status' columns to vpn session summary report in admin web portal
- Beta release of entity sync feature for Office 365
- Improved support for pipelining in IMAP4 protocol
- Add support for SNI domain matching/filtering in network attribute matching rules
- Add support for network attributes in generic proxy
- Improvements to periodic database housekeeping

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

**Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.**

# Network Box HIGHLIGHTS



## Network Box New Hardware Upgrades

Network Box is excited to announce our latest revision to the **E-Series** hardware units. In addition to an upgraded CPU, the RAM and Hard-disk capacity has been increased, with hardware RAID included as standard. These upgrades follows-on from the recent releases of the S-80i and M-255i hardware units.

For more information about the new hardware available, please follow the links below:

- S-80i: <https://network-box.com/nb5-sseries>
- M-255i: <https://network-box.com/nb5-mseries>
- E-1000i, E-2000i, and E-4000i: <https://network-box.com/nb5-eseries>



 **LINK:**  
<https://youtu.be/nMg9z5vZN-E>

### Newsletter Staff

**Mark Webb-Johnson**  
Editor

**Michael Gazeley**  
**Kevin Hla**  
Production Support

**Network Box HQ**  
**Network Box USA**  
Contributors

### Subscription

Network Box Corporation  
[nbhq@network-box.com](mailto:nbhq@network-box.com)  
or via mail at:

**Network Box Corporation**  
16th Floor, Metro Loft,  
38 Kwai Hei Street,  
Kwai Chung, Hong Kong

Tel: +852 2736-2083  
Fax: +852 2736-2778

[www.network-box.com](http://www.network-box.com)



## Network Box Media Coverage



### Brilliance Security Magazine

Bugs, Crashes, and Vulnerabilities

LINK: <https://bit.ly/2Ga5LKE>



### EME Outlook

COVID-19 and the  
Tempting Threat Landscape

LINK: <https://bit.ly/349tjHA>



### China Daily

Building up the wall  
against cybercrime

LINK: <https://bit.ly/2GiwPaq>



### Banking Today

Evolution of Business  
Continuity Plan

LINK: <https://bit.ly/349NEww>



### HPCC Hackpod Club

Hacker attack on the University  
Clinic Düsseldorf

LINK: <https://bit.ly/2S7WhBY>