What is MAC-Binding? How does it work?

MAC-Binding means binding the MAC address to the device's IP address. Think of this like assigning a name tag to every device that connects to a network.

MAC-Binding means binding the MAC address to the device's IP address. Think of this like assigning a name tag to every device that connects to a network. That way, if there's a change to your device's MAC address or IP address, you won't be able to connect to that network. With MAC-Binding, the Internet can identify and communicate with the right device, making data transmission seamless and efficient.

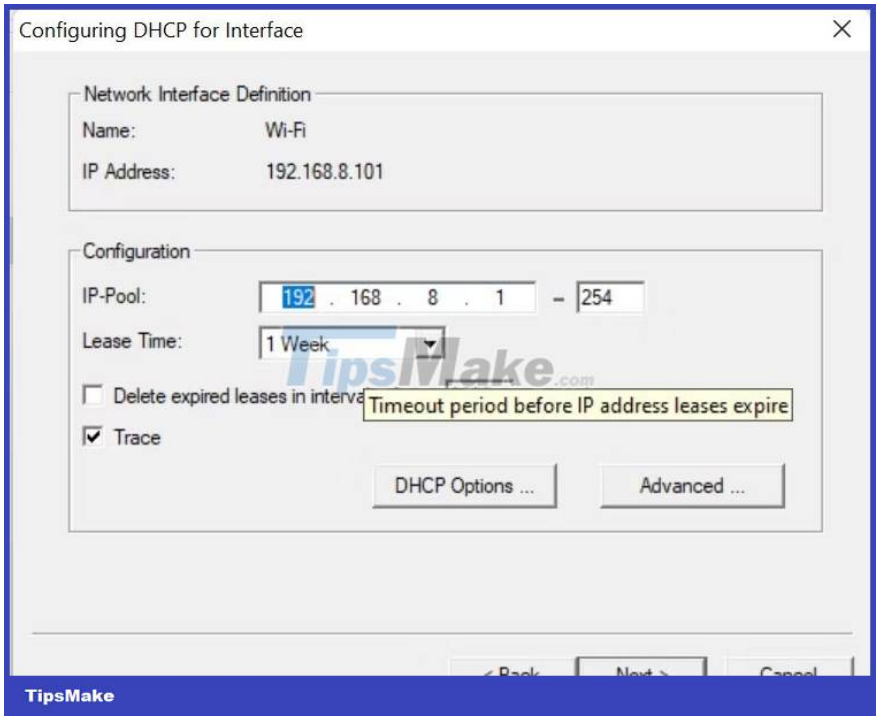
How does MAC-Binding work?

MAC-Binding allows you to "bind" an IP address to a MAC address. Once linked, the network administrator can restrict access to the network, allowing connections only from devices with specific MAC addresses.

For MAC-Binding to work successfully, the network administrator must create a list of authorized MAC addresses and their associated IP addresses on the DHCP server. This list is called the MAC-Binding table.

So, when your device requests an IP address to a DHCP server, the network administrator will go through the list to confirm if the device's MAC address is authorized and on the MAC-Binding table. After confirmation, you are assigned a corresponding IP address from the table.

The DHCP server also specifies the lease period with the IP address. If your device remains connected for the duration of the lease expiration, it will request a different IP address. After disconnecting, your device requests to release an IP address that the server can assign to another device.



In this way, MAC-Binding ensures the same IP address is assigned to a single MAC address, which helps to maintain a stable network configuration. Network administrators can also use MAC-Binding to detect a device that has performed a particular online activity.

5 advantages of MAC-Binding

MAC-Binding prevents unauthorized access to your network, as only people with approved MAC addresses are allowed access. If you change the IP or MAC address, you will not be able to access the network. Such measures make your network more stable and secure. In addition, network administrators can use MAC-Binding to track online activities on a specific device.

1. Improved security

With MAC-Binding, third-party access is not possible. Only registered MAC addresses are assigned IPs and can communicate on the network. This layer of security is useful against threat actors because it blocks unauthorized access.

2. More Control

MAC-Binding gives network administrators more control over their networks: It allows administrators to select devices that communicate on the network, blocking or restricting access to only certain devices. and limit access to sensitive data.

3. Device identification

Threat actors are becoming more elusive due to their detection techniques. But with MAC-Binding, any suspicious activity is flagged and the root device can be easily traced, as each MAC address is registered on the network's server.

4. Improve efficiency

Different devices can have the same IP address. But with MAC-Binding, the DHCP server can make sure no two devices have the same IP address. This is because each device is individually registered on the network. And by eliminating any chance of IP conflicts, improved network efficiency and connectivity increases.

5. Reserved IP address

MAC-Binding also allows network administrators to reserve IP addresses for "special" devices. This way, firewall policies can be configured and prioritized for certain devices.

The limitations and loopholes of MAC-Binding

Although MAC-Binding has many advantages, it also has some limitations and disadvantages that you should consider.

1. MAC Address Spoofing

Each MAC address comes directly with your device, assigned by the manufacturer. But the MAC address can be partially or completely changed. Bad guys use MAC address spoofing to attack wireless networks and steal sensitive information and login credentials.

2. Volatility of IP Address

After you disconnect and reconnect to the network, the device's IP address changes and threat actors can "hide" behind a particular device. This is called IP masking.

The second device can connect to the registered device and perform all online operations through that device. However, for the network, the registered device will be the only one present, with no trace of a second device. No new IP address is generated because the second device simply "masks" its IP with the IP of the registered device.

3. Limited flexibility

Your device will only be able to access the network if it is registered on the DHCP table. And while this is an extra layer of security, it can be bypassed by spoofing the MAC address to resemble the address of a registered device.

4. Manual configuration is quite complicated

MAC-Binding can be stressful and time consuming. For example, as a network administrator, you must manually register new devices in the DHCP table. In addition, you must regularly update the table as new devices are added to the network and existing devices are removed.

Although MAC-Binding adds an extra layer of security to the network, it should not be considered a complete replacement for other security measures. You can use it in conjunction with other measures such as firewalls, encryption, and access control.

MAC-Binding has many advantages and the value it offers is well worth it to ignore the existing limitations that still exist.

You finished reading the article "**What is MAC-Binding? How does it work?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
