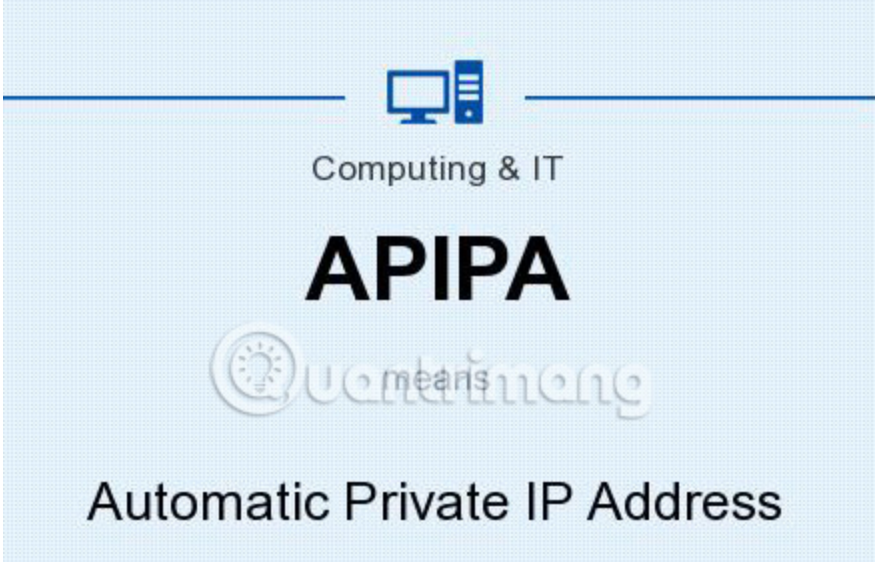
Learn about APIPA

Automatic Private IP Addressing (APIPA) is a DHCP standard, protecting computer systems from problems by creating a backup mechanism for Internet Protocol version 4 (IPv4) networks supported by Microsoft Windows.

Automatic Private IP Addressing (APIPA) is a DHCP standard, protecting computer systems from problems by creating a backup mechanism for Internet Protocol version 4 (IPv4) networks supported by Microsoft Windows. With APIPA, DHCP clients can receive IP addresses even if the DHCP server is not working. APIPA exists in all modern Windows versions, including Windows 10.

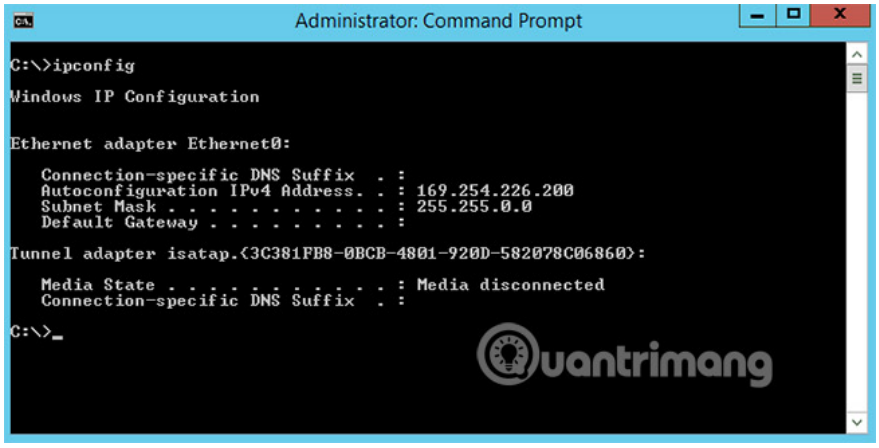
How APIPA works

Networks are set up to assign dynamic addresses based on DHCP servers to manage the set of local IP addresses available. When a Windows client tries to join the local network, it contacts the DHCP server to request its IP address. If the DHCP server stops working, causing network problems, the request cannot be performed or some problems occur on the Windows device.



When the DHCP process fails, Windows automatically assigns an IP address from its own scope (IP private), from **169.254.0.1** to **169.254.255.254.** Using the Address Resolution Protocol (ARP), client devices verify that the selected APIPA address is unique on the network before using it. The client then checks back with the DHCP server on a fixed cycle, usually every 5 minutes, and automatically updates their address when the DHCP server requests the service.

For example, when you start a computer running Windows Vista, it only waits for the DHCP server for 6 seconds before using IP from the APIPA scope. Previous versions of Windows searched for DHCP servers within three minutes.



All APIPA devices use the default network mask **255.255.0.0** and all are on the same subnet.

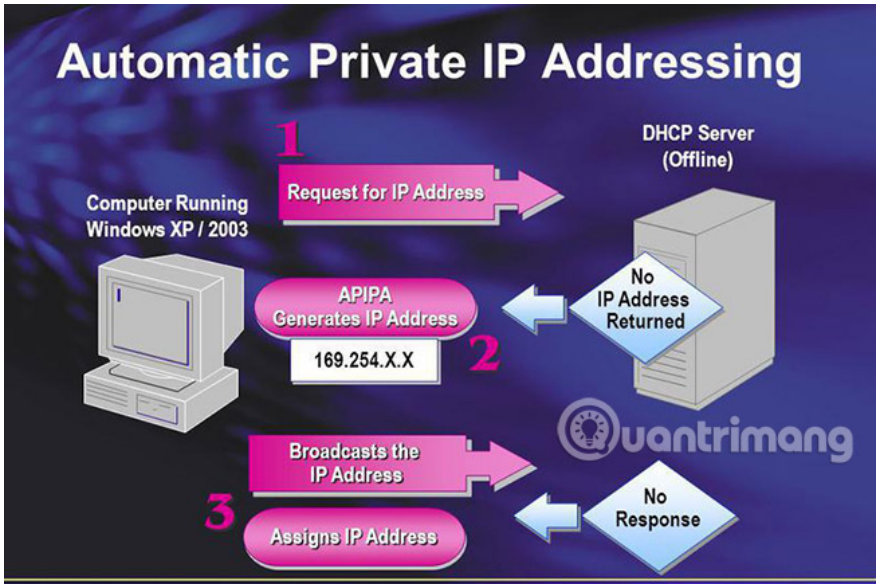
APIPA is turned on by default in Windows whenever the PC network interface is configured for DHCP. This option is called automatic configuration in Windows utilities such as **ipconfig.** Administrators can turn this feature off by editing the Windows Registry and setting the following key value to 0:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/TcpipParameters/IPAutoconfi
```

Network administrators and experienced computer users realize that errors in the DHCP process indicate network problems to identify and resolve, to help DHCP work normally.

Restrictions of APIPA

The APIPA address does not belong to any scope of private IP addresses defined by the Internet Protocol standard and is restricted to use only on local networks. Like private IP addresses, test ping or any other connection requests from the Internet and other external networks can be done directly with APIPA devices.



APIPA devices configured can communicate with peer devices on their local network but cannot communicate outside the network. Although APIPA provides Windows customers with a usable IP address, it does not provide client devices with server names (DNS or WINS) and network gateway addresses such as DHCP.

Local networks should not attempt to assign addresses manually within APIPA because IP address conflicts will occur. To maintain APIPA's benefit in pointing out DHCP errors, the admin should avoid using those addresses for any other purpose and instead limit their network to using the standard IP address range.

See more:

1. Learn about Public IP address
2. How does Dynamic NAT (dynamic NAT) and Overloading NAT work?
3. Ways to find IP Router address on Windows 10

You finished reading the article "**Learn about APIPA**" 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.