GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

P

Private IP Addressing: RFC 1918 Ranges Explained

Learn which IPv4 ranges are private, how RFC 1918 addressing works, and why CGNAT, link-local, and loopback addresses are different.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

CONTENTS

In this guide

01 What are the RFC 1918 private IP ranges?

02 How private addressing and NAT work together

03 Addresses commonly mistaken for private ranges

04 Does IPv6 use private addresses?

05 How to identify your private IP address

06 Troubleshooting private-address problems

07 Private does not mean secure

A **private IP address** identifies a device inside a local network and is not intended to be routed across the public Internet. Homes, offices, labs, and cloud networks use private addressing so many devices can communicate internally without consuming globally

unique public IPv4 addresses.

The Internet Engineering Task Force reserved three IPv4 blocks for this purpose in RFC 1918. A private address is not automatically anonymous, encrypted, or trusted: it only describes how the address is used and routed.

01 What are the RFC 1918 private IP ranges?

CIDR block	Address range	Common use
`10.0.0.0/8`	10.0.0.0–10.255.255.255	Large enterprise and cloud networks
`172.16.0.0/12`	172.16.0.0–172.31.255.255	Corporate networks and containers
`192.168.0.0/16`	192.168.0.0–192.168.255.255	Home and small-office networks

Only `172.16.0.0` through `172.31.255.255` is private; an address beginning with 172 is not automatically private. Likewise, `169.254.0.0/16` is IPv4 link-local, `127.0.0.0/8` is loopback, and `100.64.0.0/10` is shared address space for carrier-grade NAT rather than RFC 1918 space.

Only the 172.16.0.0 through 172.31.255.255 portion is private. Addresses such as 172.15.1.1 and 172.32.1.1 are not part of the RFC 1918 block.

02 How private addressing and NAT work together

A router commonly uses network address translation (NAT) to map connections from private devices to one or more public addresses. Replies return through that mapping to the correct internal device. NAT conserves public IPv4 space, but it is not a complete security control. A firewall still needs explicit rules, and applications still need authentication, encryption, and updates.

Private addresses can also appear in virtual private networks and private cloud subnets. If two connected networks use overlapping ranges, routing becomes ambiguous. Organizations should document subnets and choose non-overlapping address plans before joining networks or

acquiring another company.

03 Addresses commonly mistaken for private ranges

- `100.64.0.0/10` is shared address space used by service providers for carrier-grade NAT. It is not RFC 1918 space.
- `169.254.0.0/16` is IPv4 link-local space. A device may self-assign it when DHCP fails.
- `127.0.0.0/8` is reserved for loopback traffic to the local host.
- `0.0.0.0` has special meanings, including an unspecified address or a wildcard bind; it is not a normal device address.

04 Does IPv6 use private addresses?

IPv6 does not use the RFC 1918 blocks. Unique local addresses use `fc00::/7`, most commonly locally assigned addresses beginning with `fd`. Link-local IPv6 addresses use `fe80::/10`. IPv6 hosts may also have globally routable addresses, so firewall policy must not assume that NAT is present.

05 How to identify your private IP address

On Windows, run `ipconfig`. On Linux, use `ip address`; on macOS, use `ifconfig` or the Network settings panel. Compare the assigned address with the three RFC 1918 ranges above. Your public address, if one is used, is normally visible on the router or through an external IP-check service.

06 Troubleshooting private-address problems

1. Check the IP address, subnet prefix, default gateway, and DNS servers.
2. If the address begins with 169.254, investigate DHCP or the network connection.
3. Test the local TCP/IP stack with localhost, then test the gateway.

4. Look for overlapping subnets when a VPN connects but internal resources remain unreachable.
5. Review NAT and firewall rules instead of assuming a private address is blocked or safe by default.

07 Private does not mean secure

Attackers, compromised devices, malicious browser extensions, and misconfigured cloud services can all operate inside private networks. Segment sensitive systems, use least-privilege access, encrypt important traffic, patch exposed services, and monitor internal activity. Addressing is part of network design; it is not a substitute for security.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com