Configure Multiple IP Addresses for AIQ IP Spoofing

Configure Multiple IP Addresses for AIQ IP Spoofing

Last reviewed: September 21, 2026

This article explains the maintenance considerations for adding multiple source IP addresses for AIQ performance testing. Treat IP spoofing as an advanced network configuration that must be coordinated with infrastructure owners.

When to use this guidance

- A performance test requires traffic to originate from multiple source IPs.
- The test node host and network route tables support additional addresses.
- Network, firewall, and monitoring teams have approved the source ranges.

Recommended approach

1. Confirm the IP range, subnet mask, gateway, and routing requirements with the network team.

2. Apply the additional addresses on the test node host using the operating-system network tooling approved for that environment.
3. Restart or refresh only the services required for the OS to recognize the new addresses.
4. Run a small validation scenario and confirm traffic appears from the expected addresses.
5. Document the range and remove temporary addresses when testing is complete.

Note: Do not enable IP spoofing on shared hosts without network approval; misconfigured source addresses can disrupt routing or monitoring.

Last updated: October 16, 2026

Revision #4
Created 2026-07-31 15:38:47 UTC by Admin
Updated 2026-10-16 18:19:13 UTC by mmora