P

# Promiscuous Mode: What it does on a network interface

What it is Promiscuous mode is a network-interface setting that passes all frames the interface can see to the operating system instead of only frames addressed to that interface. Administrators and security tools use it for packet...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

## What it is

Promiscuous mode is a network-interface setting that passes all frames the interface can see to the operating system instead of only frames addressed to that interface. Administrators and security tools use it for packet capture, troubleshooting, intrusion detection, and monitoring. The mode itself is a capability, not malware.

## How it works

Capture software requests the mode through the operating system and records traffic visible to that interface. On a modern switched network, a normal endpoint usually sees broadcasts and its own traffic, not every other host's packets. A network tap, mirror port, wireless monitor setup, compromised switch, or local position may expose more traffic.

## Key points

- Promiscuous mode does not bypass encryption; HTTPS and properly protected protocols still hide message contents.
- Unauthorized packet capture can expose unencrypted credentials, metadata, and sensitive internal traffic.
- The setting can be legitimate on monitoring servers and suspicious on an ordinary user workstation.

## Safe administration

- Authorize captures, define their scope, and protect packet files as sensitive data.
- Monitor unexpected capture drivers, tools, interface changes, and mirror-port configuration.
- Use encrypted protocols so intercepted network traffic is less useful.
- Investigate context before disabling the mode on systems that provide approved monitoring.