IP Settings

- Summary
- IPv4 Settings
- IPv6 Settings

Summary

Several IPv4 and IPv6 related kernel and system-wide parameters are configurable.

IPv4 Settings

Sub-menu: `/ip settings`

Property	Description
accept-redirects (*yes | no*; Default: **no**)	Whether to accept ICMP redirect messages. Typically should be enabled on a host and disabled on routers.
accept-source-route (*yes | no*; Default: **no**)	Whether to accept packets with the SRR option. Typically should be enabled on the router.
allow-fast-path (*yes | no*; Default: **yes**)	Allows Fast Path.
arp-timeout (*time interval*; Default: **30s**)	Sets Linux **base_reachable_time** (base_reachable_time_ms) on all interfaces that use ARP. The initial validity of the ARP entry is picked from the interval [timeout/2 - 3*timeout/2] (default from 15s to 45s) after the neighbor was found. Can use postfix ms, s, m, h, d for milliseconds, seconds, minutes, hours, or days. if no postfix is set then seconds (s) are used. The parameter means how long a valid ARP record will be considered complete if no one communicates with the specific MAC/IP during this time. The parameter does not represent a time when an ARP entry is removed from the ARP cache (see **max-neighbor-entries** setting).
icmp-rate-limit (*integer [0..4294967295]*; Default: **10**)	Limit the maximum rates for sending ICMP packets whose type matches icmp-rate-mask to specific targets. **0** disables any limiting, other values indicate the minimum space between responses in milliseconds.
icmp-rate-mask (*[0..FFFFFFFF]*; Default: **0x1818**)	Mask made of ICMP types for which rates are being limited. More info in Linux man pages
ip-forward (*yes | no*; Default: **yes**)	Enable/disable packet forwarding between interfaces. Resets all configuration parameters to defaults according to RFC1812 for routers.

rp-filter (*loose | no | strict*; Default: **no**)	Disables or enables source validation. - no - No source validation. - strict - Strict mode as defined in RFC3704 Strict Reverse Path. Each incoming packet is tested against the FIB and if the interface is not the best reverse path the packet check will fail. By default failed packets are discarded. - loose - Loose mode as defined in RFC3704 Loose Reverse Path. Each incoming packet's source address is also tested against the FIB and if the source address is not reachable via any interface the packet check will fail. The current recommended practice in RFC3704 is to enable strict mode to prevent IP spoofing from DDoS attacks. If using asymmetric routing or other complicated routing or VRRP, then the loose mode is recommended. **Warning:** strict mode does not work with routing tables
secure-redirects (*yes | no*; Default: **yes**)	Accept ICMP redirect messages only for gateways, listed in the default gateway list.
send-redirects (*yes | no*; Default: **yes**)	Whether to send ICMP redirects. Recommended to be enabled on routers.
tcp-syncookies (*yes | no*; Default: **no**)	Send out syncookies when the syn backlog queue of a socket overflows. This is to prevent the common 'SYN flood attack'. syncookies seriously violate TCP protocol, and disallow the use of TCP extensions, which can result in serious degradation of some services (f.e. SMTP relaying), visible not by you, but to your clients and relays, contacting you.
max-neighbor-entries (*integer [0..4294967295]*; Default:)	Sets Linux **gc_thresh3.** A maximum number of allowed neighbors in the ARP table. Since RouterOS version 7.1, the default value depends on the installed amount of RAM. It is possible to set a higher value than the default, but it increases the risk of out-of-memory condition. The default values for certain RAM sizes: - 2048 for 64 MB, - 4096 for 128 MB, - 8192 for 256 MB, - 16384 for 512 MB or higher. The ARP cache stores ARP entries, and if some of these entries are incomplete, they can stay in the cache for an indefinite period of time. This will only happen if the number of entries in the cache is less than one-fourth of the maximum number allowed. The reason for this is to prevent the unnecessary running of the garbage-collector when the ARP table is not close to being full.
route-cache (*yes | no*; Default: **yes**)	Disable or enable the Linux route cache. Note that disabling the route cache, will also disable the fast path.

Read-Only Properties

Property	Description
ipv4-fast-path-active (*yes | no*)	Indicates whether fast-path is active
ipv4-fast-path-bytes (*integer*)	Amount of fast-pathed bytes
ipv4-fast-path-packets (*integer*)	Amount of fast-pathed packets
ipv4-fasttrack-active (*yes | no*)	Indicates whether fasttrack is active
ipv4-fasttrack-bytes (*integer*)	Amount of fasttracked bytes
ipv4-fasttrack-packets (*integer*)	Amount of fasttracked packet.

IPv6 Settings

Sub-menu: `/ipv6 settings`

Changing /ipv6 settings will not dynamically remove the old SLAAC configuration present on your router. A reboot is required to apply the new settings.

Property	Description
accept-redirects (*no | yes-if-forwarding-disabled*; Default: **yes-if-forwarding-disabled**)	Whether to accept ICMP redirect messages. Typically should be enabled on the host and disabled on routers
accept-router-advertisements (*no | yes | yes-if-forwarding-disabled*; Default: **yes-if-forwarding-disabled**)	Accept router advertisement (RA) messages. If enabled, the router will be able to get the address using stateless address configuration
disable-ipv6 (*yes | no*; Default: **no**)	Enable/disable system wide IPv6 settings (prevents LL address generation)
forward (*yes | no*; Default: **yes**)	Enable/disable packet forwarding between interfaces
max-neighbor-entries (*integer [0..4294967295]*; Default:)	A maximum number or IPv6 neighbors. Since RouterOS version 7.1, the default value depends on the installed amount of RAM. It is possible to set a higher value than the default, but it increases the risk of out-of-memory condition. The default values for certain RAM sizes: • 1024 for 64 MB, • 2048 for 128 MB, • 4096 for 256 MB, • 8192 for 512 MB, • 16384 for 1024 MB or higher.