NAME

network_namespaces – overview of Linux network namespaces

DESCRIPTION

Network namespaces provide isolation of the system resources associated with networking: network devices, IPv4 and IPv6 protocol stacks, IP routing tables, firewall rules, the */proc/net* directory (which is a symbolic link to */proc/PID/net*), the */sys/class/net* directory, various files under */proc/sys/net*, port numbers (sockets), and so on. In addition, network namespaces isolate the UNIX domain abstract socket namespace (see **unix**(7)).

A physical network device can live in exactly one network namespace. When a network namespace is freed (i.e., when the last process in the namespace terminates), its physical network devices are moved back to the initial network namespace (not to the namespace of the parent of the process).

A virtual network (**veth**(4)) device pair provides a pipe-like abstraction that can be used to create tunnels between network namespaces, and can be used to create a bridge to a physical network device in another namespace. When a namespace is freed, the **veth**(4) devices that it contains are destroyed.

Use of network namespaces requires a kernel that is configured with the **CONFIG_NET_NS** option.

SEE ALSO

nsenter(1), **unshare**(1), **clone**(2), **veth**(4), **proc**(5), **sysfs**(5), **namespaces**(7), **user_namespaces**(7), **brctl**(8), **ip**(8), **ip–address**(8), **ip–link**(8), **ip–netns**(8), **iptables**(8), **ovs–vsctl**(8)