NAME

ip-vrf − run a command against a vrf

SYNOPSIS

ip vrf { *COMMAND* | **help** }

ip vrf show [*NAME*]

ip vrf identify [*PID*]

ip vrf pids *NAME*

ip vrf exec [*NAME*] *command*...

DESCRIPTION

A VRF provides traffic isolation at layer 3 for routing, similar to how a VLAN is used to isolate traffic at layer 2. Fundamentally, a VRF is a separate routing table. Network devices are associated with a VRF by enslaving the device to the VRF. At that point network addresses assigned to the device are local to the VRF with host and connected routes moved to the table associated with the VRF.

A process can specify a VRF using several APIs -- binding the socket to the VRF device using SO_BINDTODEVICE, setting the VRF association using IP_UNICAST_IF or IPV6_UNICAST_IF, or specifying the VRF for a specific message using IP_PKTINFO or IPV6_PKTINFO.

By default a process is not bound to any VRF. An association can be set explicitly by making the program use one of the APIs mentioned above or implicitly using a helper to set SO_BINDTODEVICE for all IPv4 and IPv6 sockets (AF_INET and AF_INET6) when the socket is created. This ip-vrf command is a helper to run a command against a specific VRF with the VRF association inherited parent to child.

ip vrf show [NAME] - Show all configured VRF

This command lists all VRF and their corresponding table ids. If NAME is given, then only that VRF and table id is shown. The latter command is useful for scripting where the table id for a VRF is needed.

ip vrf exec [NAME] cmd ... - Run cmd against the named VRF

This command allows applications that are VRF unaware to be run against a VRF other than the default VRF (main table). A command can be run against the default VRF by passing the "default" as the VRF name. This is useful if the current shell is associated with another VRF (e.g, Management VRF).

This command requires the system to be booted with cgroup v2 (e.g. with systemd, add systemd.unified_cgroup_hierarchy=1 to the kernel command line).

This command also requires to be ran as root or with the CAP_SYS_ADMIN, CAP_NET_ADMIN and CAP_DAC_OVERRIDE capabilities. If built with libcap and if capabilities are added to the ip binary program via setcap, the program will drop them as the first thing when invoked, unless the command is vrf exec.
NOTE: capabilities will NOT be dropped if CAP_NET_ADMIN is set to INHERITABLE to avoid breaking programs with ambient capabilities that call ip. Do not set the INHERITABLE flag on the ip binary itself.

ip vrf identify [PID] - Report VRF association for process

This command shows the VRF association of the specified process. If PID is not specified then the id of the current process is used.

ip vrf pids NAME - Report processes associated with the named VRF

This command shows all process ids that are associated with the given VRF.

CAVEATS

This command requires a kernel compiled with CGROUPS and CGROUP_BPF enabled.

The VRF helper *only* affects network layer sockets.

EXAMPLES

ip vrf exec red ssh 10.100.1.254

Executes ssh to 10.100.1.254 against the VRF red table.

SEE ALSO

ip(8), **ip-link**(8), **ip-address**(8), **ip-route**(8), **ip-neighbor**(8)

AUTHOR

Original Manpage by David Ahern