In this chapter, detailed description of NF chaining mechanism in kernel space is given. The architecture makes use of existing Netfilter subsystem in Linux. First, the role of Netfilter system in the network stack is explained. Second, the main structure of Kernel-based NFCI is described in Sec. 4.2. This NFCI consists of identification of flows and NF chaining mechanism.

Netfilter: Overview Netfilter is software inside the Linux 2.4.x and later kernel series, which enables packet filtering and packet mangling. It is a set of hooks that are placed in several stages in network stack and in each hook multiple kernel modules can be registered. Each of the kernel modules will work as a NF, such as Firewall and NAT. Figure fig: netfilter$_systemshowsthenetworkstackandfivenetfilterhooksembeddedinsideit.Thebottom$
$itemize$

P RE_ROUTING : This hook is triggered by incoming packet soon after entering the network stack. This is processed before the packet reaches the routing subsystem.

L OCAL_IN : This hook is processed after the packet has been routed and is destined to the local host.

F ORWARD : This hook is processed after the packet has been routed and is to be forwarded to another host.

L OCAL_OUT : This hook is triggered by locally created packet as soon as it enters the stack.

P OST_ROUTING : This is the last hook that the outgoing or transmitted packet passes before being put out on the wire.