Manual:Packet Flow

From MikroTik Wiki

Contents

Applies to RouterOS: v3, v4, v5+

Overview

MikroTik RouterOS is designed to be easy to operate in various aspects of network configuration. Therefore creating limitation for individual IP or natting internal clients to a public address or Hotspot configuration can be done without the knowledge about how the packets are processed in the router - you just go to corresponding menu and create necessary configuration.

However more complicated tasks, such as traffic prioritization, routing policies, where it is necessary to utilize more than one RouterOS facility, requires knowledge: How these facilities work together? What happens when and why?

To address these questions we created a packet flow diagram.

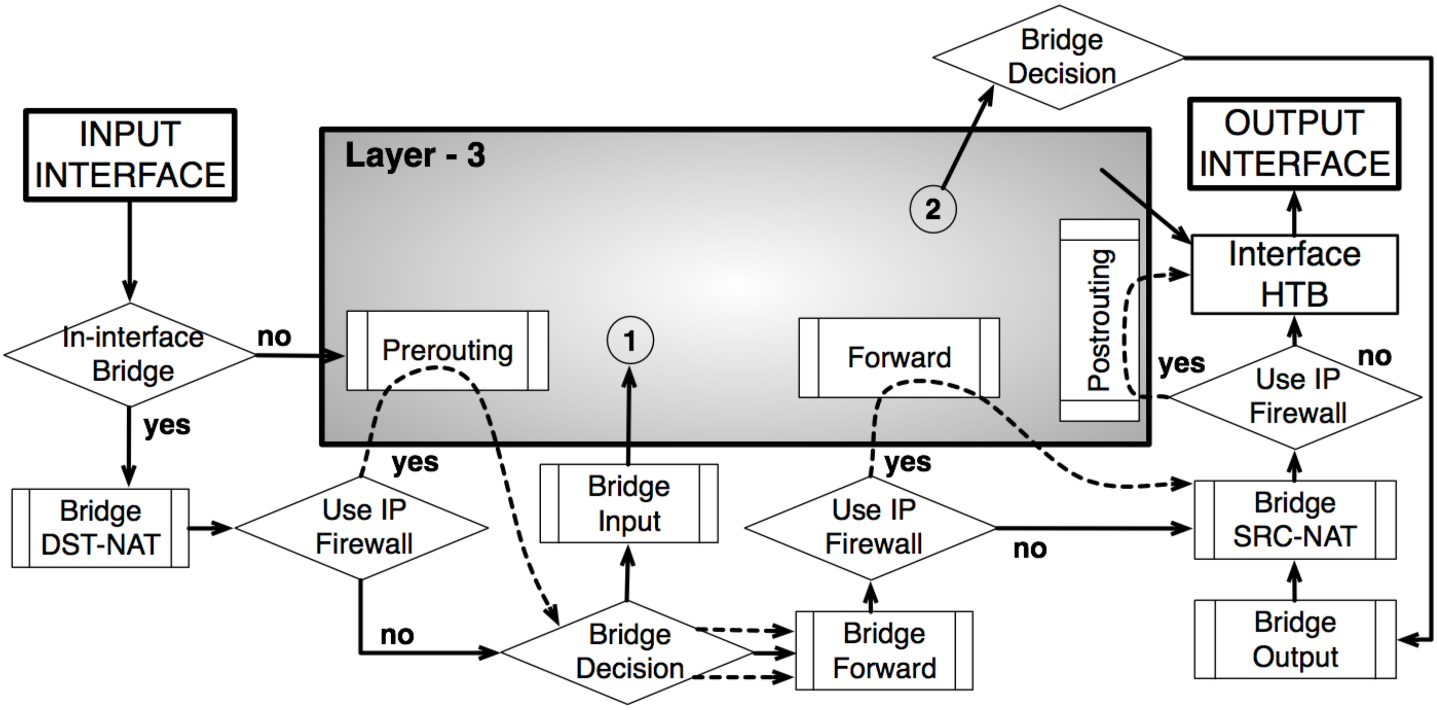
Diagram

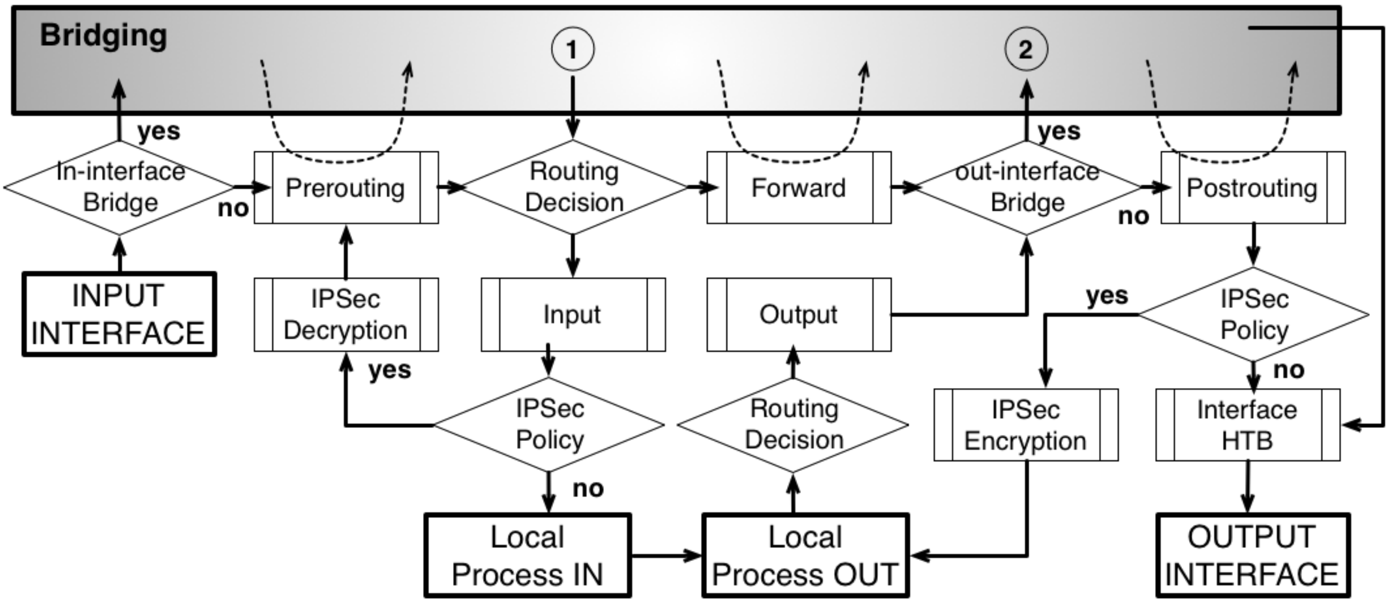
Note: a new diagram has been created, specifically optimized for the new mechanisms in RouterOS v6 and above. Please see it here

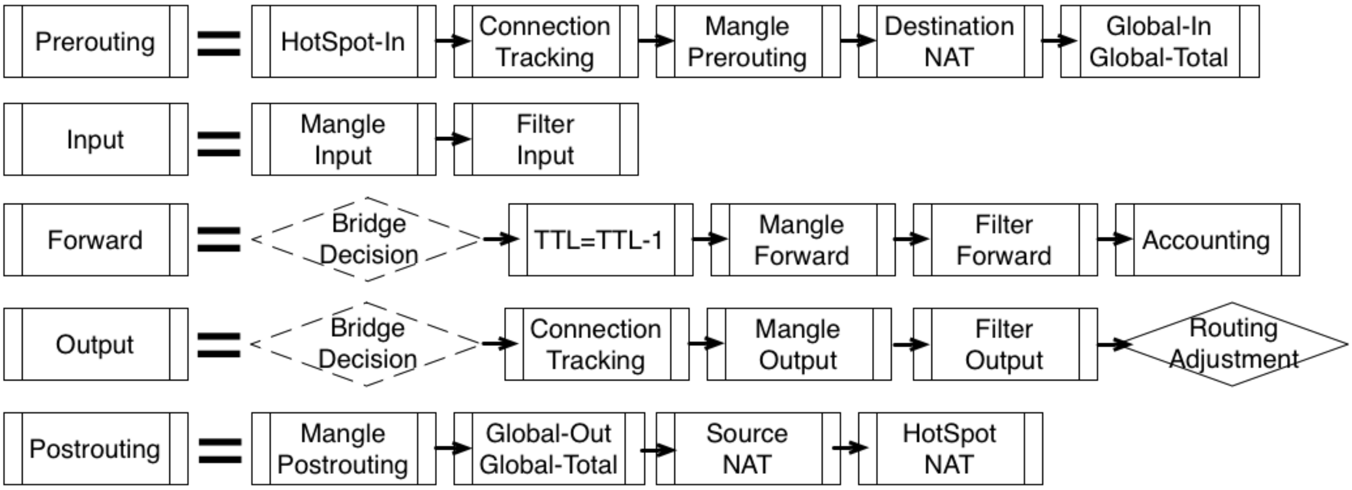
As it was impossible to get everything in one diagram, **Packet flow diagram** for Mikrotik RouterOS v3.x was created in 2 parts:

- **Bridging or Layer-2 (MAC)** where Routing part is simplified to one "Layer-3" box
- **Routing or Layer-3 (IP)** where Bridging part is simplified to one "Bridging" box

The packet flow diagram is also available as a PDF (http://wiki.mikrotik.com/images/1/1b/Traffic_Flow_Diagram_RouterOS_3.x.pdf).

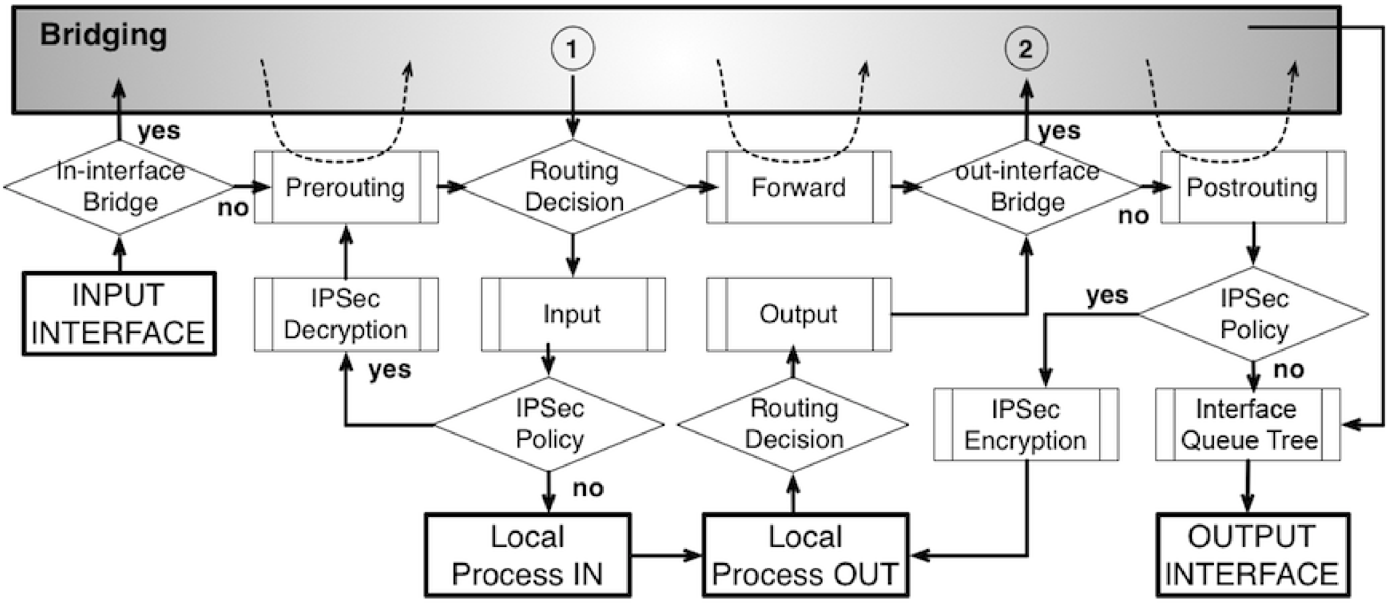


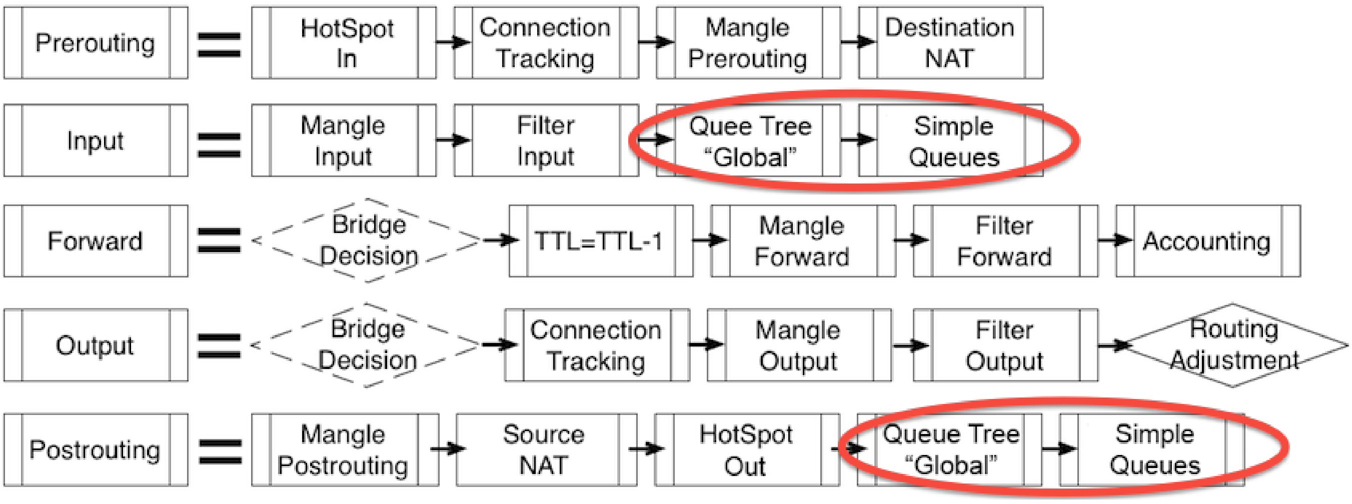




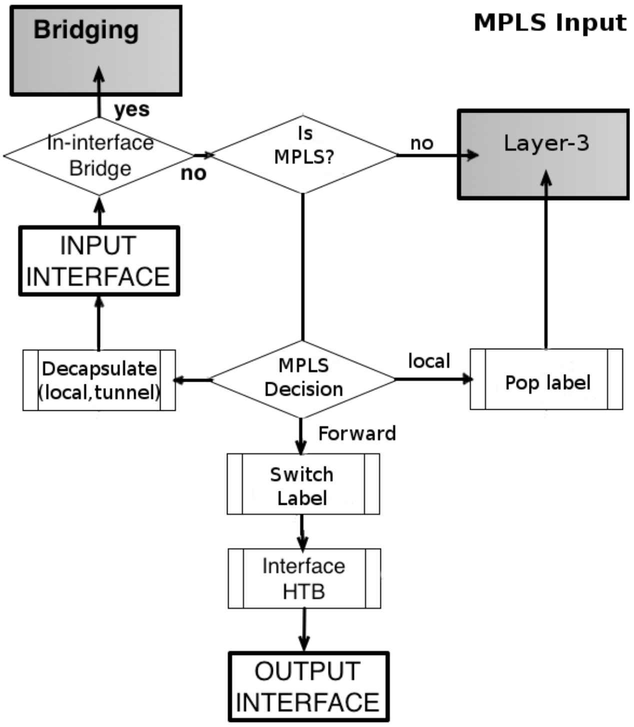
Changes in RouterOS v6

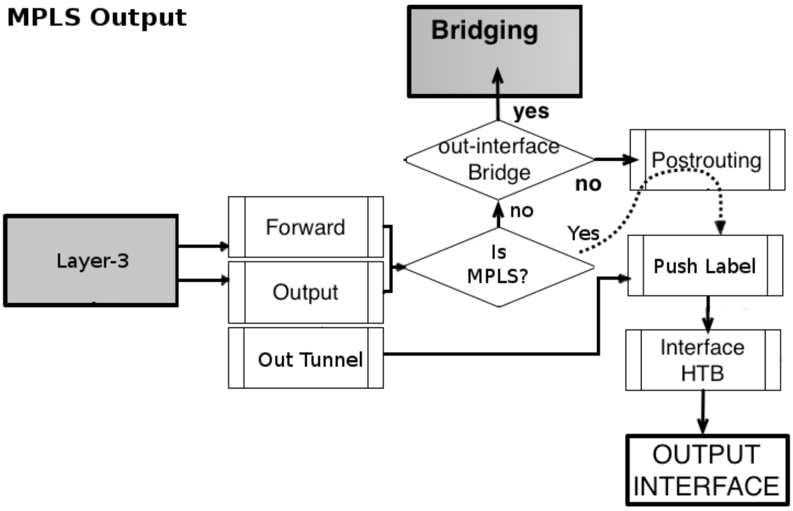
The following changes have been made to the Packet Flow in RouterOS v6, see red cirdled elements in the image:





MPLS Packet Flow





Analysis

Basic Concepts

INPUT INTERFACE - starting point in packets way through the router facilities. It does not matter what interface (physical or virtual) packet is received it will start its way from here.

OUTPUT INTERFACE - last point in packets way through the router facilities. Just before the packet is actually sent out.

[Local Process IN] - last point in packets way **to** router itself, after this packet is discarded

[Local Process OUT] - starting point for packets generated by router itself

Configurable Facilities

Each and every facilities in this section corresponds with one particular menu in RouterOS. Users are able to access those menu and configure these facilities directly

[Connection Tracking] - **/ip firewall connection tracking**

[Filter Input] [Filter Forward] [Filter Output] - **/ip firewall filter**

[Source NAT] [Destination NAT] - **/ip firewall nat**

[Mangle Prerouting] [Mangle Input] [Mangle Forward] [Mangle Output] [Mangle Postrouting] - **/ip firewall mangle**

[Global-In Global-Total] [Global-Out Global-Total] [Interface HTB] - **/queue simple** and **/queue tree**

◇ IPSec Policy - **/ip ipsec policy**

[Accounting] - **/ip accounting**

◇ Use IP Firewall - **/interface bridge settings** - available only for traffic that go **through** the bridge. For all other traffic default value is **Yes**

Bridge Input | Bridge Forward | Bridge Output - **/interface bridge filter**

Bridge DST-NAT | Bridge SRC-NAT - **/interface bridge nat**

Automated processes and decisions

In-interface Bridge - check if the *actual input interface* is a port for bridge OR checks if *input interface* is bridge

HotSpot-In - allow to capture traffic witch otherwise would be discarded by connection tracking - this way our Hotspot feature are able to provide connectivity even if networks settings are in complete mess

Bridge Decision - bridge goes through the MAC address table in order to find a match to destination MAC address of packet. When match is found - packet will be send out via corresponding bridge port. In case of no match - multiple copies of packet will be created and packet will be sent out via all bridge ports

Bridge Decision - this is a workaround, allows to use "out-bridge-port" before actual bridge decision.

Routing Decision - router goes through the route n order to find a match to destination IP address of packet. When match is found - packet will be send out via corresponding port or to the router itself . In case of no match - packet will be discarded.

Routing Adjustment - this is a workaround that allows to set-up policy routing in mangle chain output

TTL=TTL-1 - indicates exact place where Time To Live (TTL) of the routed packet is reduced by 1. If it become 0 packet will be discarded

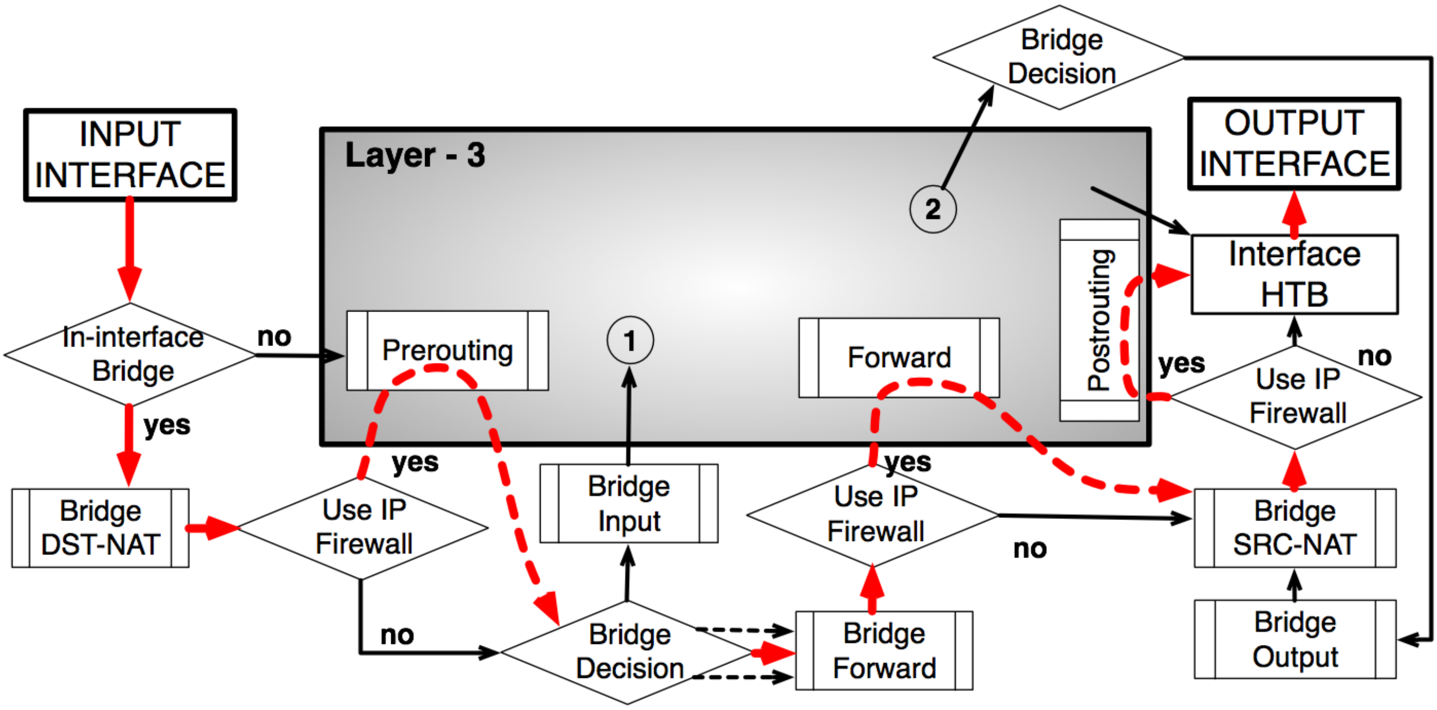
IPSec Decryption IPSec Encryption - self explainatory

out-interface Bridge - check if the *actual output interface* is a port for bridge OR checks if *output interface* is bridge

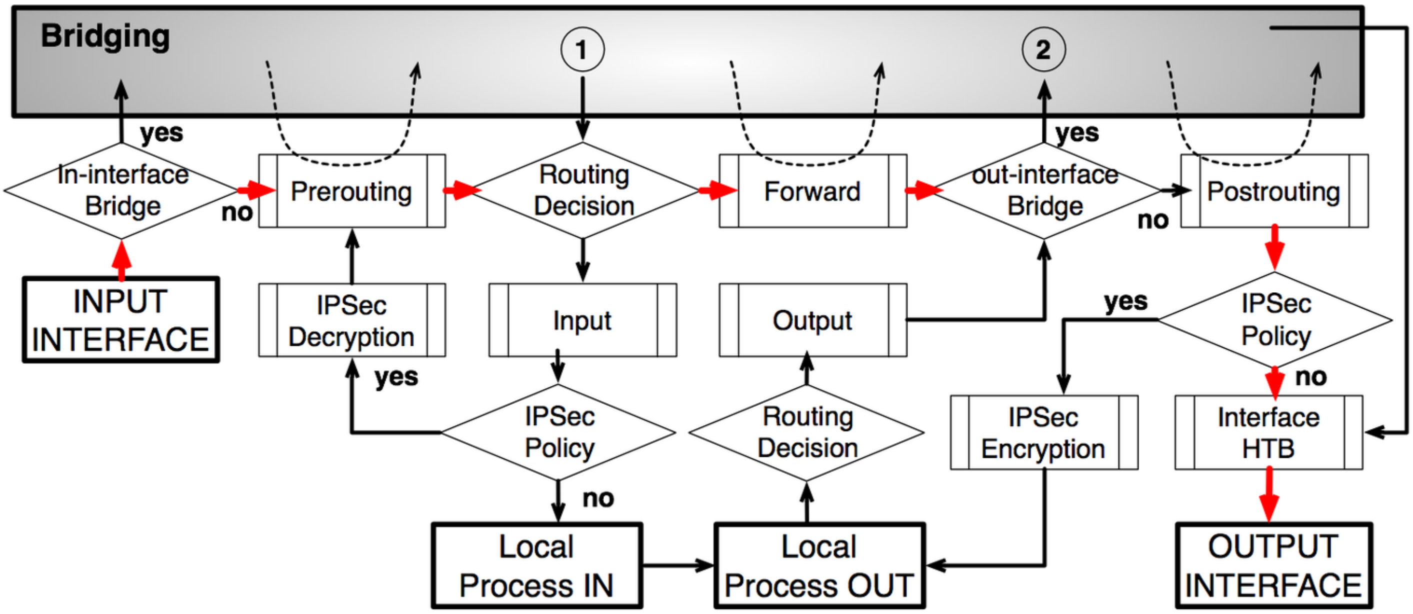
HotSpot-Out - undo all that was done by hotspot-in for the packets that is going back to client.

Examples

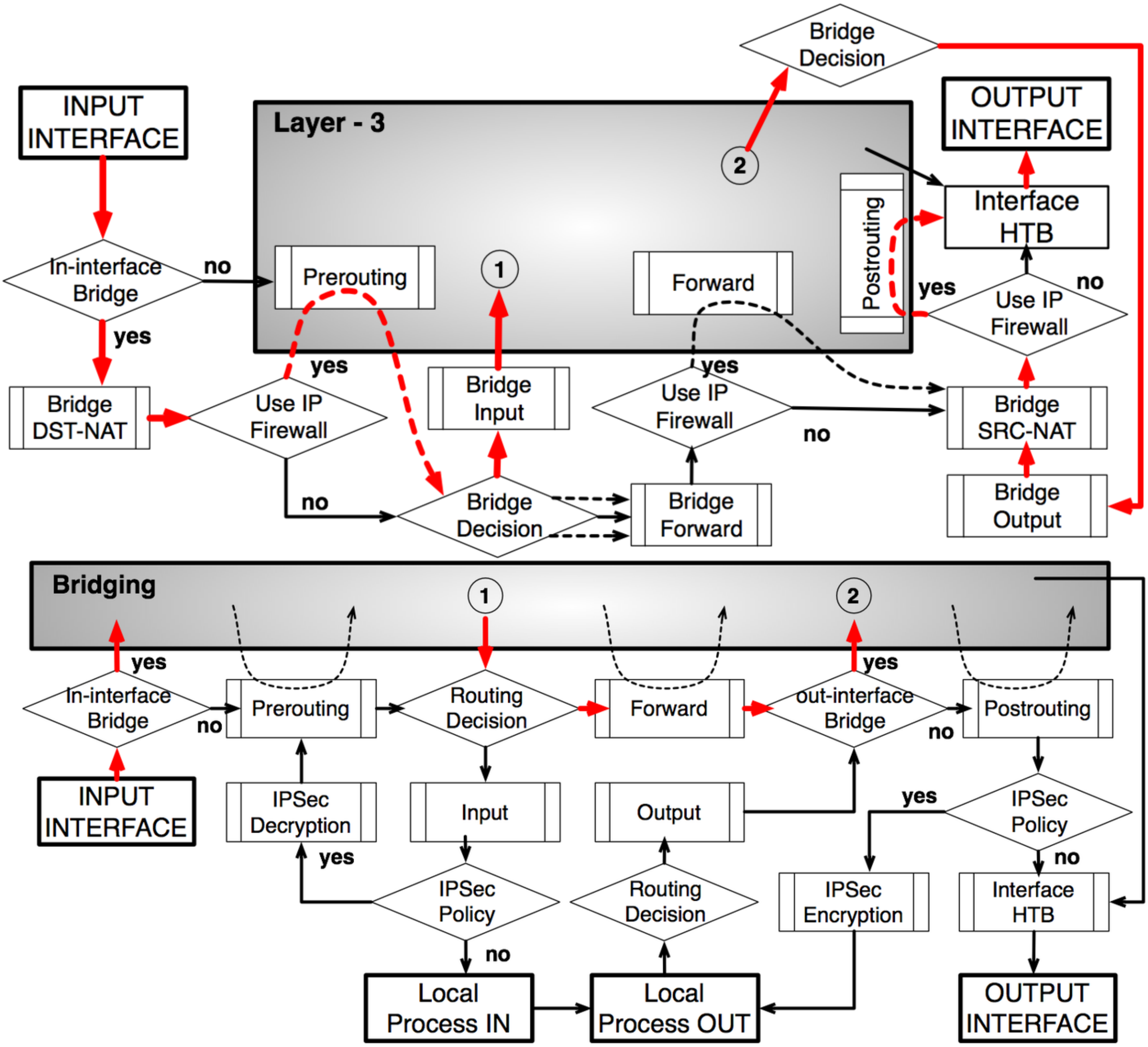
Bridging with use-ip-firewall=yes



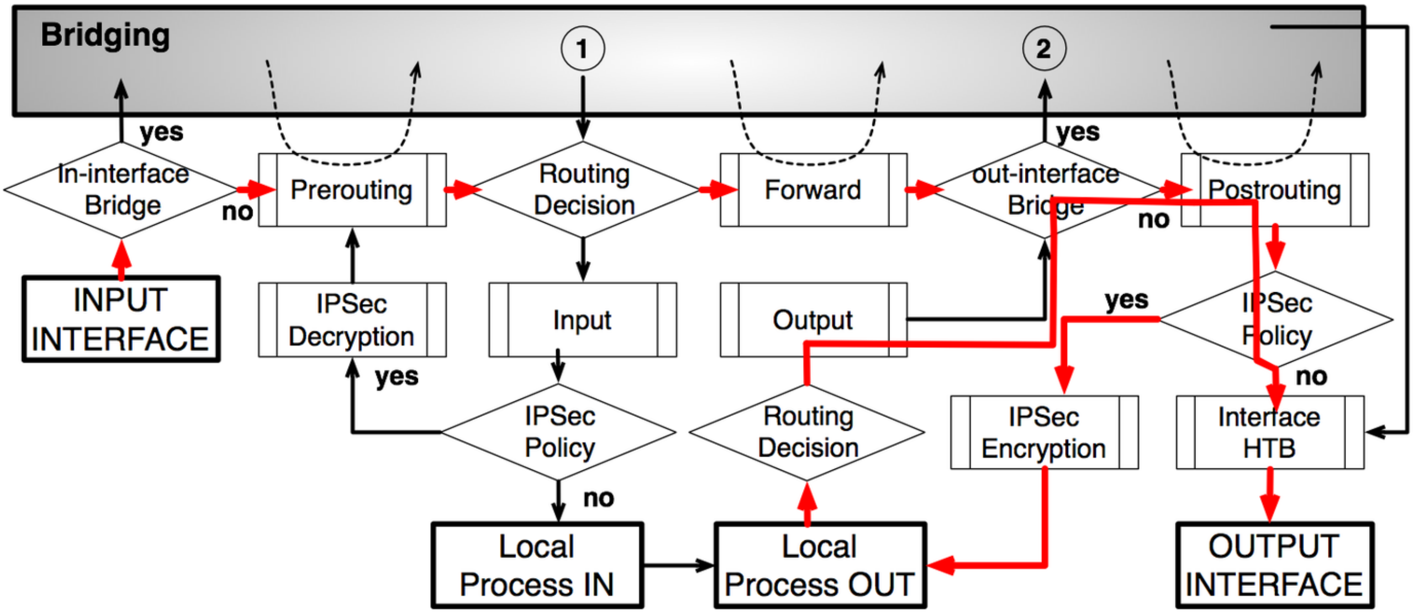
Routing - from Ethernet to Ethernet interface



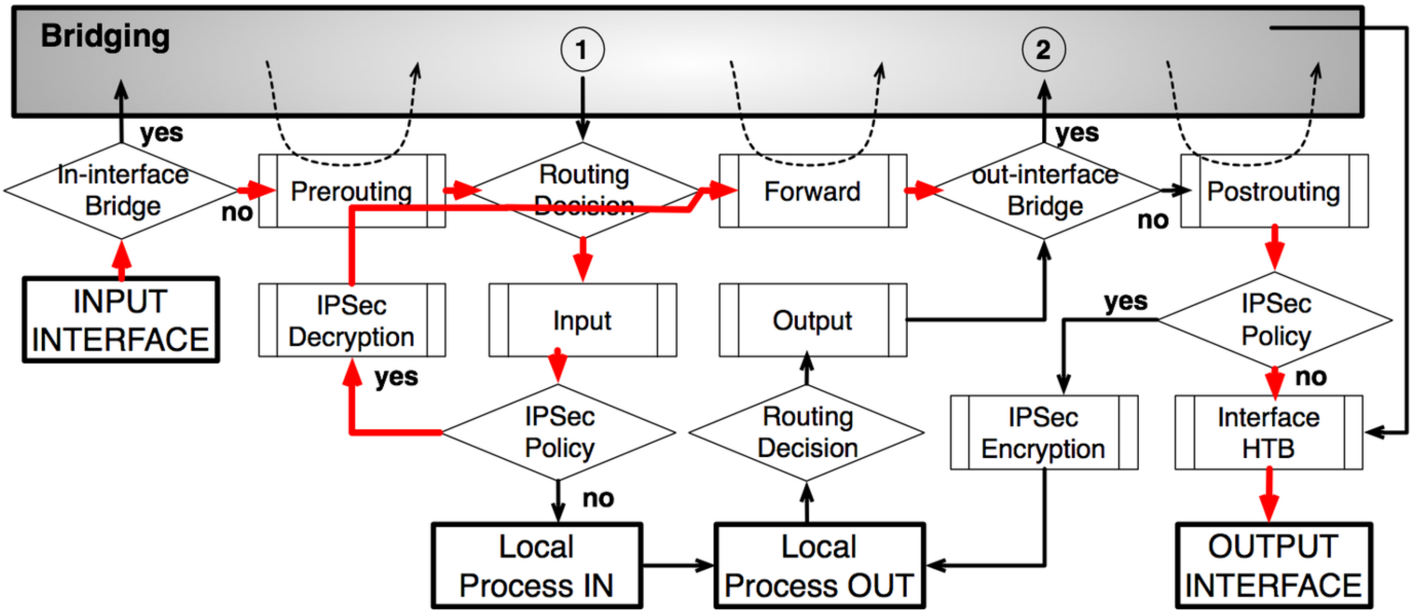
Routing from one Bridge interface to different Bridge interface



IPsec encryption



IPsec decryption



Retrieved from "https://wiki.mikrotik.com/index.php?title=Manual:Packet_Flow&oldid=28467"

Categories: Manual | IP | QoS | Case Studies

- This page was last edited on 2 June 2016, at 13:41.