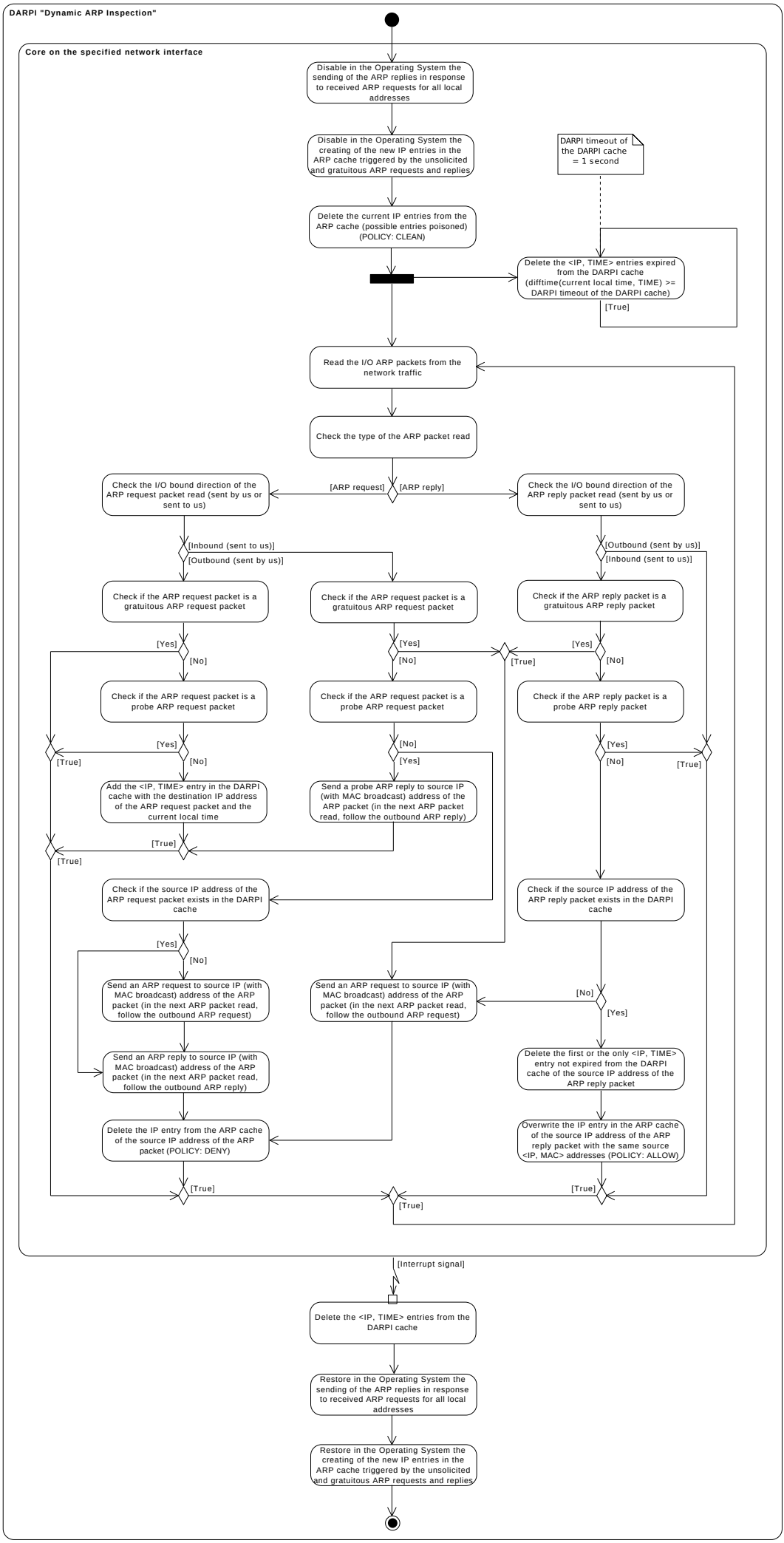
DARPI "Dynamic ARP Inspection"
Core on the specified network interface
Disable in the Operating System the sending of the ARP replies in response to received ARP requests for all local addresses
Disable in the Operating System the creating of the new IP entries in the ARP cache triggered by the unsolicited and gratuitous ARP requests and replies
Delete the current IP entries from the ARP cache (possible entries poisoned) (POLICY: CLEAN)
DARPI timeout of the DARPI cache = 1 second
Delete the <IP, TIME> entries expired from the DARPI cache (difftime(current local time, TIME) >= DARPI timeout of the DARPI cache)
[True]
Read the I/O ARP packets from the network traffic
Check the type of the ARP packet read
[ARP request]
[ARP reply]
Check the I/O bound direction of the ARP request packet read (sent by us or sent to us)
Check the I/O bound direction of the ARP reply packet read (sent by us or sent to us)
[Inbound (sent to us)]
[Outbound (sent by us)]
[Outbound (sent by us)]
[Inbound (sent to us)]
Check if the ARP request packet is a gratuitous ARP request packet
Check if the ARP request packet is a gratuitous ARP request packet
Check if the ARP reply packet is a gratuitous ARP reply packet
[Yes]
[No]
[Yes]
[No]
[True]
[Yes]
[No]
Check if the ARP request packet is a probe ARP request packet
Check if the ARP request packet is a probe ARP request packet
Check if the ARP reply packet is a probe ARP reply packet
[Yes]
[No]
[True]
[No]
[Yes]
[No]
[Yes]
[True]
Add the <IP, TIME> entry in the DARPI cache with the destination IP address of the ARP request packet and the current local time
Send a probe ARP reply to source IP (with MAC broadcast) address of the ARP packet (in the next ARP packet read, follow the outbound ARP reply)
[True]
[True]
Check if the source IP address of the ARP request packet exists in the DARPI cache
Check if the source IP address of the ARP reply packet exists in the DARPI cache
[Yes]
[No]
Send an ARP request to source IP (with MAC broadcast) address of the ARP packet (in the next ARP packet read, follow the outbound ARP request)
Send an ARP request to source IP (with MAC broadcast) address of the ARP packet (in the next ARP packet read, follow the outbound ARP request)
[No]
[Yes]
Send an ARP reply to source IP (with MAC broadcast) address of the ARP packet (in the next ARP packet read, follow the outbound ARP reply)
Delete the first or the only <IP, TIME> entry not expired from the DARPI cache of the source IP address of the ARP reply packet
Delete the IP entry from the ARP cache of the source IP address of the ARP packet (POLICY: DENY)
Overwrite the IP entry in the ARP cache of the source IP address of the ARP reply packet with the same source <IP, MAC> addresses (POLICY: ALLOW)
[True]
[True]
[True]
[Interrupt signal]
Delete the <IP, TIME> entries from the DARPI cache
Restore in the Operating System the sending of the ARP replies in response to received ARP requests for all local addresses
Restore in the Operating System the creating of the new IP entries in the ARP cache triggered by the unsolicited and gratuitous ARP requests and replies