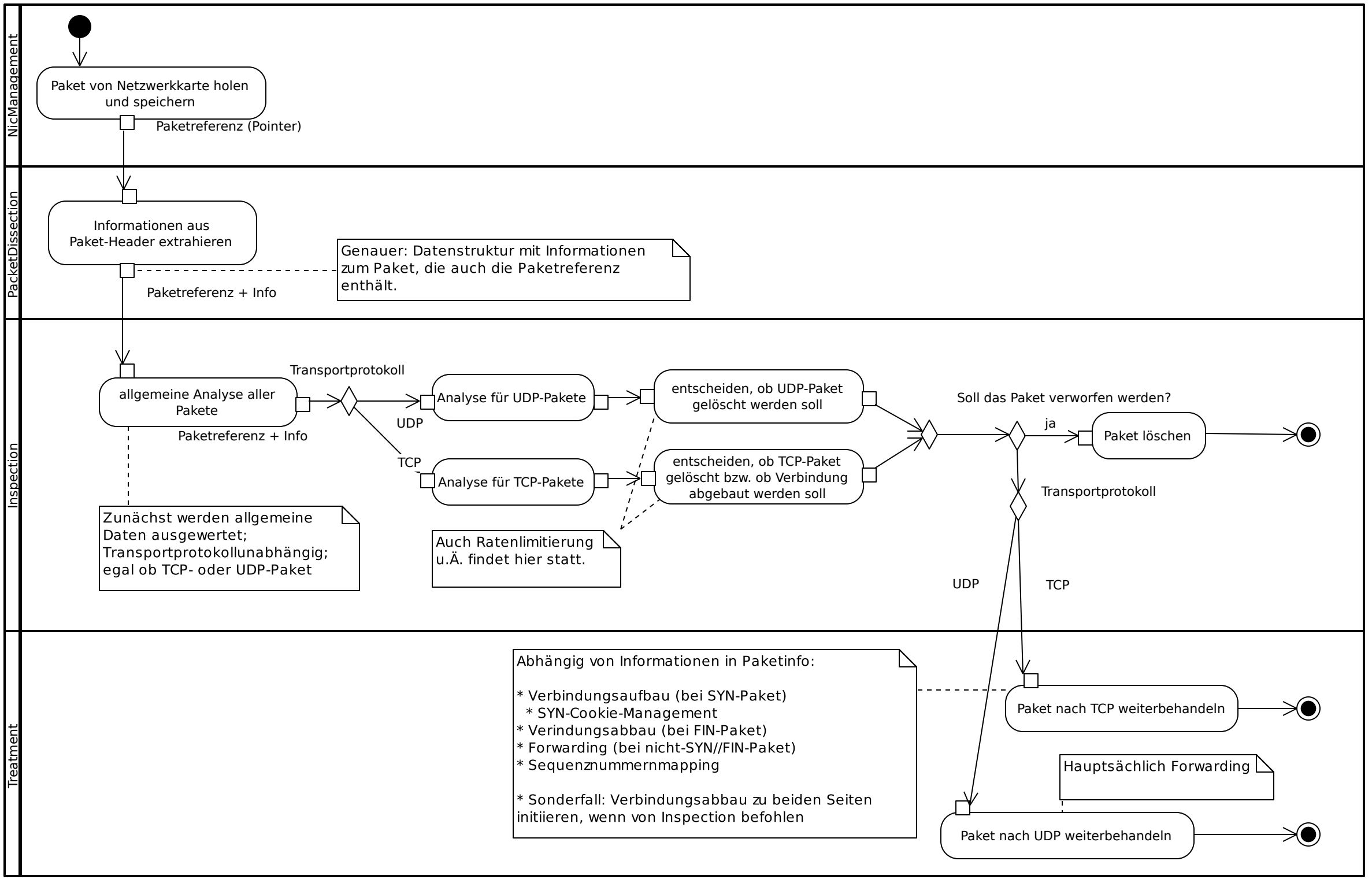
NicManagement
Paket von Netzwerkkarte holen und speichern
Paketreferenz (Pointer)
PacketDissection
Informationen aus Paket-Header extrahieren
Genauer: Datenstruktur mit Informationen zum Paket, die auch die Paketreferenz enthält.
Paketreferenz + Info
Inspection
allgemeine Analyse aller Pakete
Paketreferenz + Info
Transportprotokoll
UDP
TCP
Analyse für UDP-Pakete
Analyse für TCP-Pakete
entscheiden, ob UDP-Paket gelöscht werden soll
entscheiden, ob TCP-Paket gelöscht bzw. ob Verbindung abgebaut werden soll
Auch Ratenlimitierung u.Ä. findet hier statt.
Zunächst werden allgemeine Daten ausgewertet; Transportprotokollunabhängig; egal ob TCP- oder UDP-Paket
Soll das Paket verworfen werden?
ja
Paket löschen
Transportprotokoll
UDP
TCP
Treatment
Abhängig von Informationen in Paketinfo:
* Verbindungsaufbau (bei SYN-Paket)
* SYN-Cookie-Management
* Verindungsabbau (bei FIN-Paket)
* Forwarding (bei nicht-SYN//FIN-Paket)
* Sequenznummernmapping
* Sonderfall: Verbindungsabbau zu beiden Seiten initiieren, wenn von Inspection befohlen
Paket nach TCP weiterbehandeln
Hauptsächlich Forwarding
Paket nach UDP weiterbehandeln