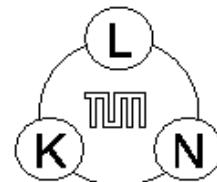


Automatische Topologieerkennung und -Überwachung in Intranets

Marie-Mélisande Tromparent

Tromparent@ei.tum.de

Lehrstuhl für Kommunikationsnetze, TU München
Univ.-Prof. Dr.-Ing. Jörg Eberspächer



Einführung

- Heutige IP-Netze: immer größer und komplexer
 - Manuelle Erfassung der Netztopologie oft sehr aufwendig
 - Aktuellste Topologie benötigt für den effizienten Netzbetrieb
- => Forschungsthema „Automatische Topologieerkennung“
- => Erkennung von Netzänderungen von größter Bedeutung

In diesem Beitrag:

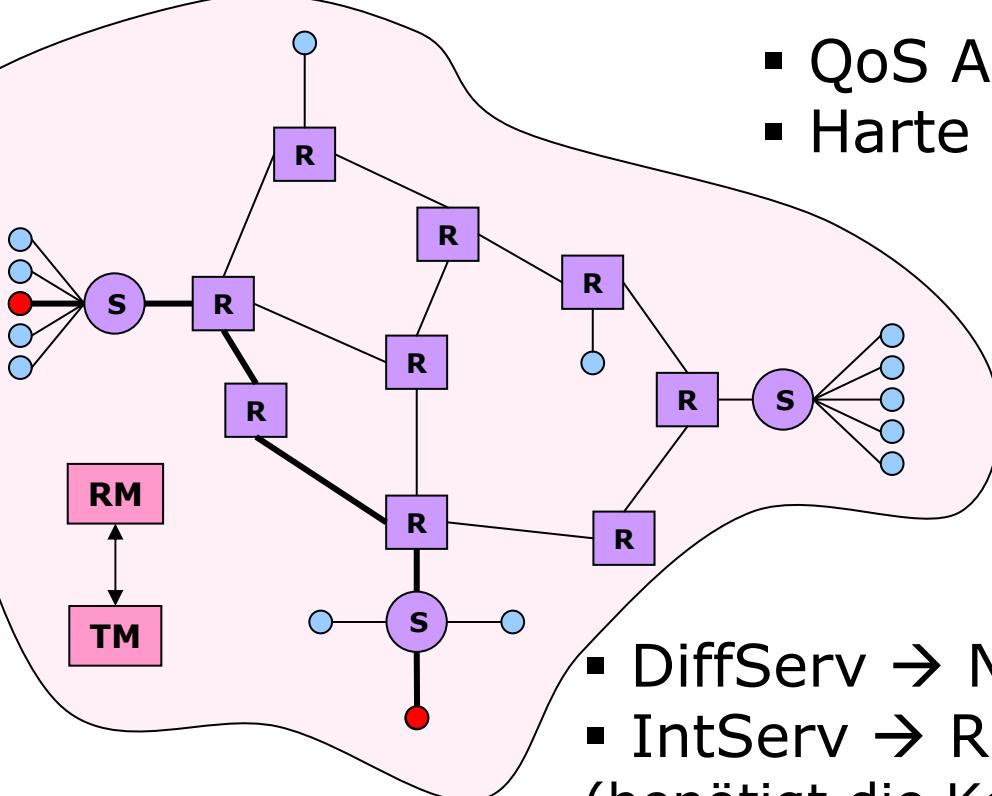
- Topologieerkennung: Definition und einige existierende Ansätze
- Beschreibung des am LKN entwickelten Topology-Managers (TM)
 - Anwendungsbereich und Annahmen
 - Ablauf der Ersttopologieerkennung
 - Überwachung der Netztopologie
 - Ausblick: Erkennung von WLAN Stationen

Die hier vorgestellte Arbeit ist im Rahmen eines Forschungsprojekts in Kooperation mit der **Siemens AG** entstanden (ICN EN HS D 11)

Topologieerkennung - Definition

- Definition abhängig vom Anwendungsbereich !
- Bestimmung des aus den Netzknoten und deren Verbindungen bestehenden Graphen
 - Varianten:
 - Erkennung von Schicht 3 – Netzknoten
 - Erkennung von Schicht 2 & 3 – Netzknoten
 - Erfassung zusätzlicher Informationen
 - Unterschiedliche Anwendungsbereiche:
 - Öffentliches Internet
 - Firmennetze / Intranet
- Existierende Ansätze
 - Internet Control Message Protocol (ICMP, „ping“ and „traceroute“ Funktionen)
 - Simple Network Management Protocol (SNMP)
 - DNS zone transfer

Ressourcenmanagement Architektur



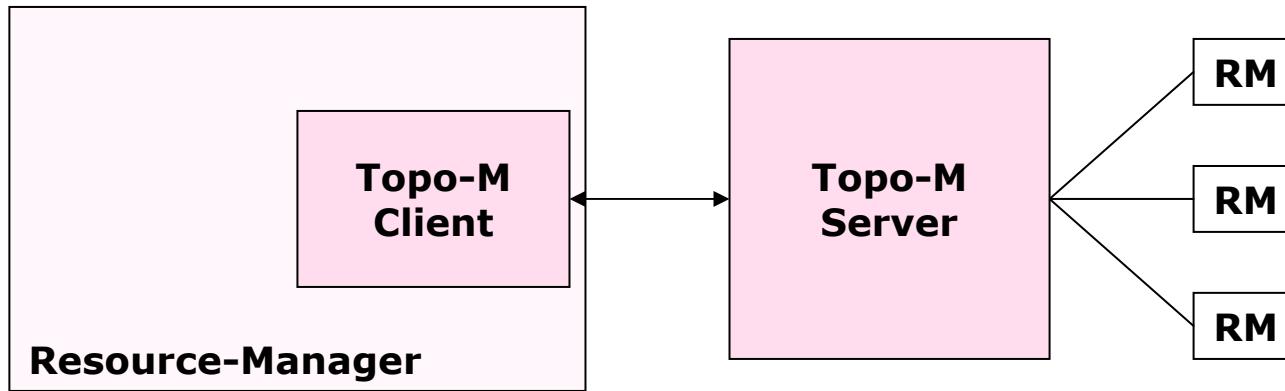
- QoS Architektur
- Harte und weiche QoS Garantien
- Firmennetze
- DiffServ → Netz mit Dienstklassen
- IntServ → Ressourcenreservierung
(benötigt die Kenntnis der Netztopologie)

RM: Resource-Manager

TM: Topology-Manager

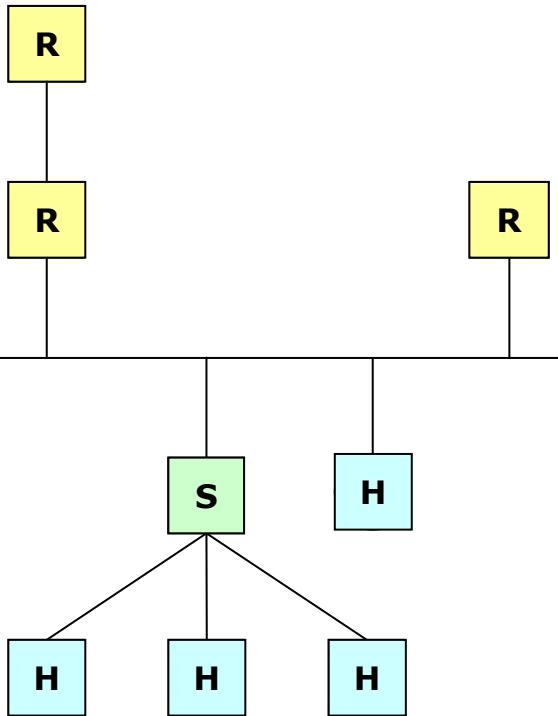
Topology-Manager - Overview

- Client/Server Architektur



- Entwicklung unter MS-Windows
- Verwendete Software-Komponenten: Net-SNMP Bibliothek, Standard Template Library (STL) und Microsoft Foundation Classes

Topology-Manager Server



1. Bestimmung des Subnetzes
2. Bestimmung aller gültigen IP Adressen
3. Ping nach allen IP Adressen
4. Klassifizierung der Knoten → SNMP
5. Erfassung zusätzlicher Informationen
6. Bearbeitung der nächsten Subnetzen

=> **Aufbau der Topologiekarte**

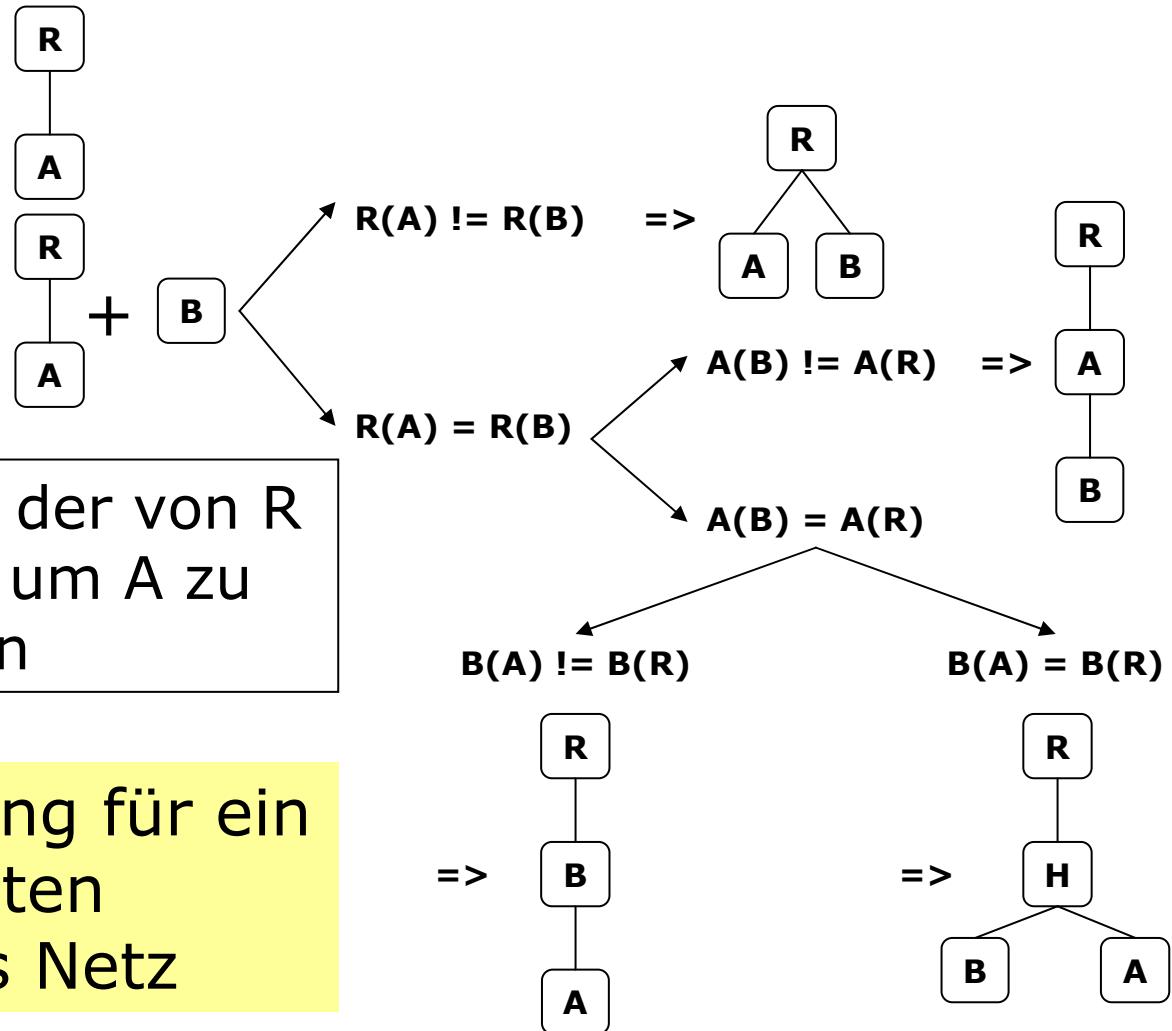
Topology-Manager Server

1. Fall: 2 Knoten

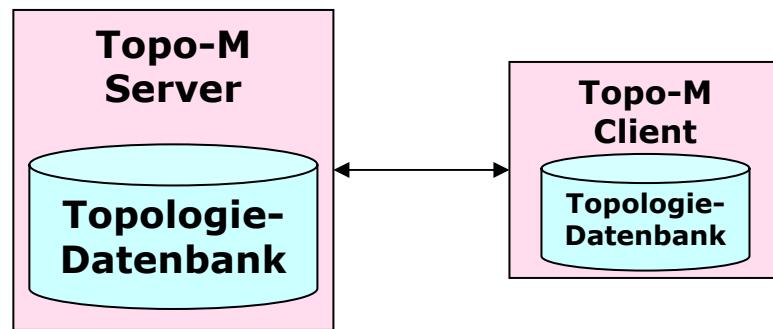
2. Fall: 3 Knoten

Def: $R(A)$ = Port, der von R verwendet wird um A zu erreichen

Verallgemeinerung für ein aus n Knoten bestehendes Netz



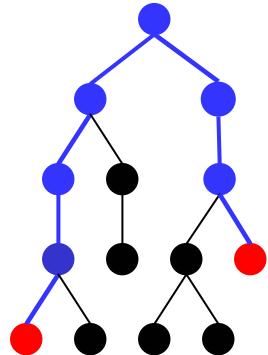
Topology-Manager Client



- Lokale Kopie der Topologiedatenbank
- Schnittstelle zum RM: QueryRoute

Suche nach dem Routing-Pfad

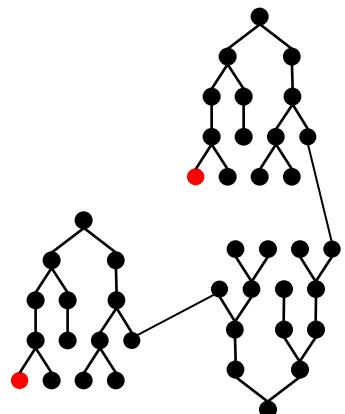
Schicht 2 Suche



Schicht 3 Suche

=> Routingtabelle
der Router des
Netzes

Kombination



Überwachung der Netztopologie

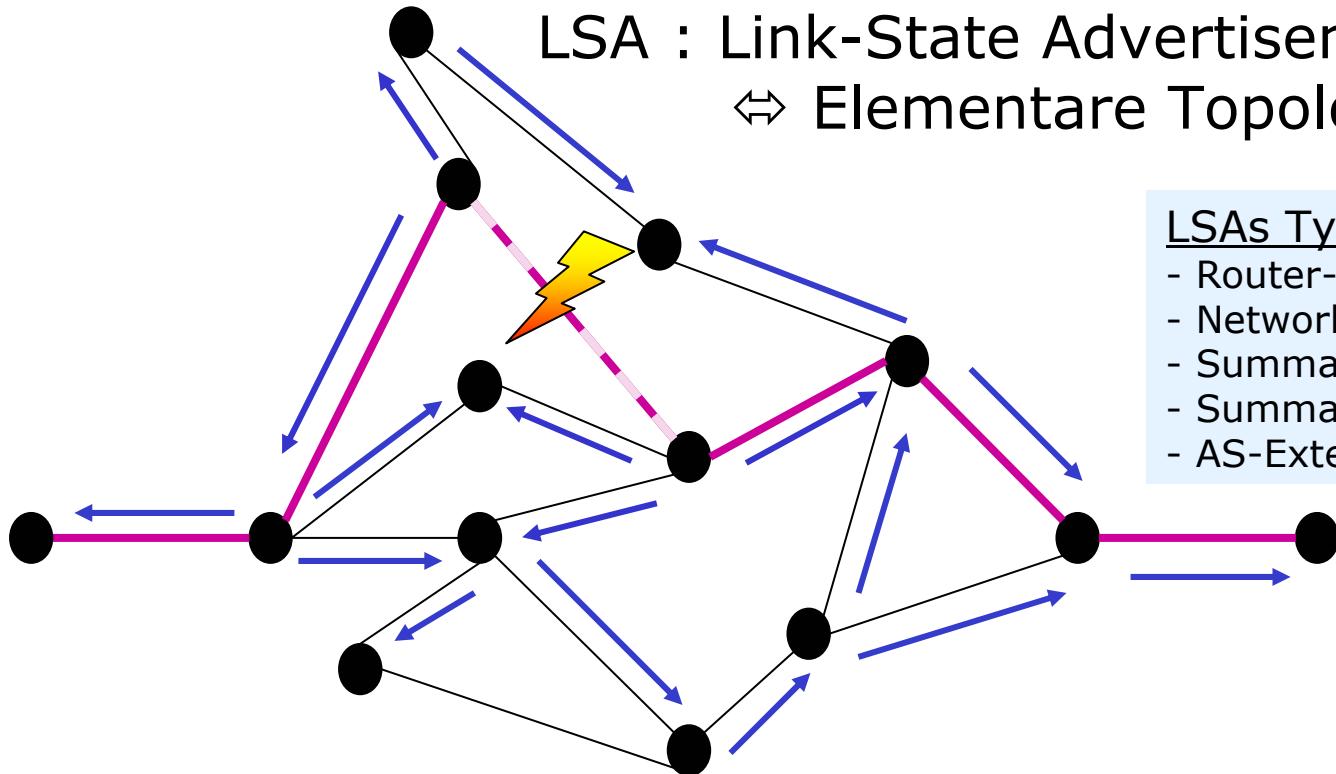
- Relevante Netzänderungen
 - Ausfälle (Knoten oder Link)
 - Einführung neuer Netzkomponenten (Knoten oder Link)
 - Konfigurationsänderungen (Metrik des Routing Protokolls, Bandbreite oder Puffergröße pro Dienstklasse, usw.)
- Kein Mechanismus, der alle Änderungen detektieren kann
=> Kombination
- Mögliche Ansätze
 - Polling Verfahren
 - SNMP Traps
 - OSPF basiertes Verfahren

OSPF basiertes Verfahren

LSU : Link-state Update Packet

$$\text{LSU} = \sum \text{LSAs}$$

LSA : Link-State Advertisement
 \Leftrightarrow Elementare Topologie Information

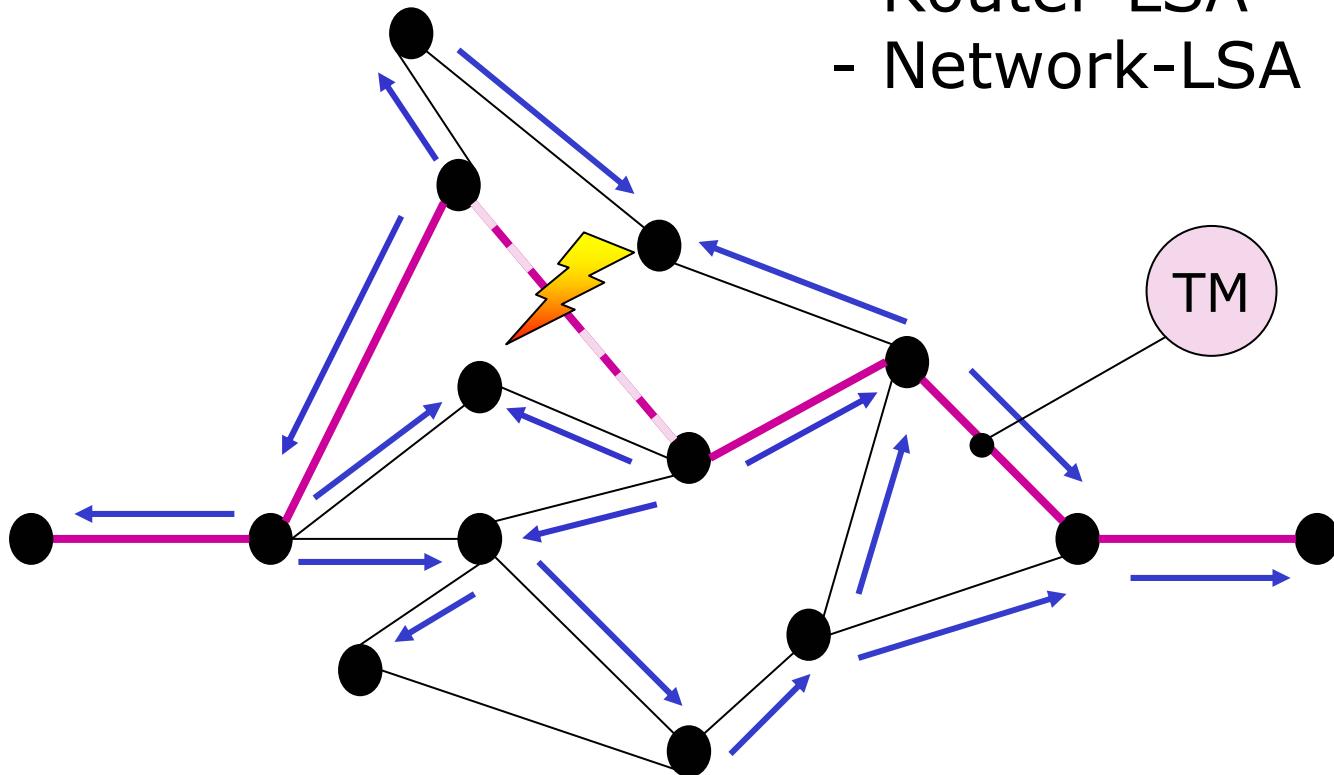


LSAs Typen:

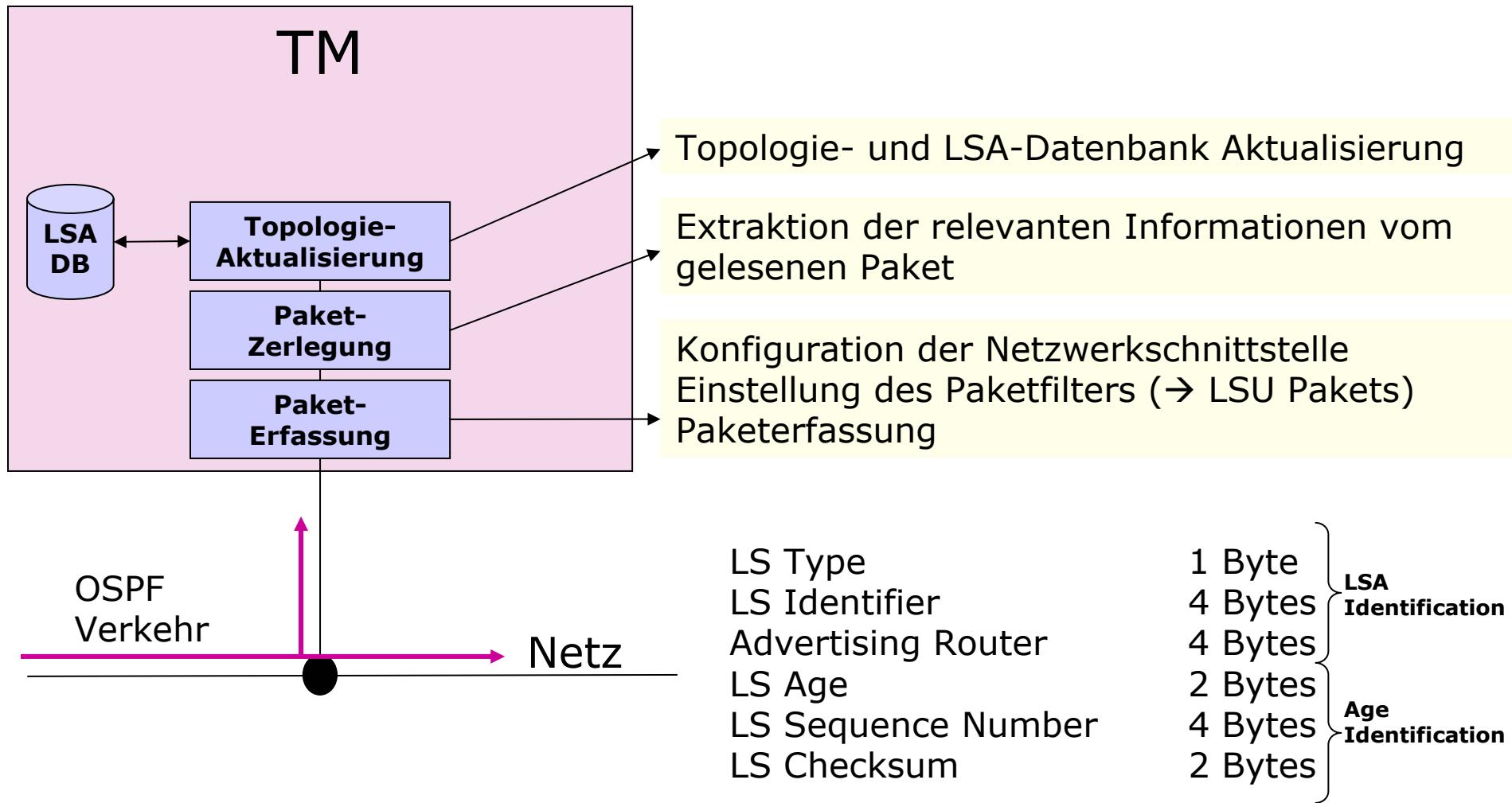
- Router-LSA
- Network-LSA
- Summary-LSA (IP network)
- Summary-LSA (AS Border Router)
- AS-External-LSA

OSPF basiertes Verfahren

- TM irgendwo ans Netz angeschlossen
- Belauschen der OSPF Nachrichten
 - Router-LSA
 - Network-LSA



OSPF basiertes Verfahren



Zusammenfassung

- Automatische Topologieerkennung
 - Anwendungsbereich: Ressourcenmanagement Architektur
 - Beschreibung des Topology-Managers
- Automatische Topologieüberwachung
 - Mechanismen zur Erkennung von Netzänderungen
 - OSPF-basiertes Verfahren
- Ausblick
 - Korrekte Erkennung von weiteren Geräten
 - VLAN-Erkennung
 - Erkennung von WLAN-Benutzern