Automatische Topologieerkennung und –Überwachung in Intranets

Marie-Mélisande Tromparent
Lehrstuhl für Kommunikationsnetze, Technische Universität München
mm.tromparent@tum.de

Dieser Beitrag berichtet von einer am Lehrstuhl für Kommunikationsnetze der TU München durchgeführten Forschungsarbeit, die sich mit dem Thema Automatische Topologieerkennung und –Überwachung in Intranets beschäftigt. Um heutige IP-Netze leichter und effizienter betreiben zu können, ist es von Vorteil, ihre genaue Topologie zu kennen. Da IP-Netze immer größer und komplexer werden, ist eine manuelle Topologieerkennung sehr aufwendig. Es ist noch aufwendiger die Topologiesicht auf dem Laufenden zu halten. Dadurch werden die zahlreichen Forschungsarbeiten im Bereich „Automatische Topologieerkennung“ rechtfertigt.

Abhängig vom Verwendungszweck und –Kontext gibt es unterschiedliche Methoden, um Topologieerkennung zu realisieren: Das *Internet Control Message Protocol* (ICMP) ermöglicht zum Beispiel die Schicht 3 Topologieerkennung basierend auf *ping* oder *traceroute* Funktionsaufrufen. Nachteil dieser Methode ist, dass aus Sicherheitsgründen nicht alle Netzknoten solche Anfragen beantworten. Außerdem wird die Schicht 2 Topologie dadurch nicht erkannt. Das *Simple Network Management Protocol* (SNMP) wird auch häufig im Kontext der Topologieerkennung verwendet. Es basiert auf der Abfrage von besonderen Datenbanken (MIB, *Management Information Base*), die autorisierten Benutzern neben topologischen Informationen zusätzliche Konfigurationsdaten zur Verfügung stellen.

In diesem Beitrag wird eine mögliche Realisierung eines Topologieerkennungsdienstes vorgestellt, die im Kontext von Firmennetzen (Intranets) entstanden ist. Dadurch konnte angenommen werden, dass die für die Topologieerkennung zuständige Instanz (*Topology-Manager*, TM) über privilegierte Zugangsrechte zu den Netzknoten verfügt. Nach einem beispielhaften Anwendungsbereich wird die Funktionsweise des TMs präsentiert: Erkennung und Klassifizierung der aktiven Netzknoten, spezifisches Abfragen von gezielten Netzknoten und die Bereitstellung der gesammelten Information. Da Topologieerkennung nur Sinn macht, wenn die Topologiesicht aktuell gehalten werden kann, werden anschließend Mechanismen präsentiert, womit Netzänderungen detektiert werden können (*Polling*, SNMP *Traps*, Belauschen des Routing Protokolls). Als Ausblick wird noch das Problem der Erkennung und Überwachung von Wireless LANs Teilnehmern kurz behandelt.

Die hier vorgestellte Arbeit ist im Rahmen eines Forschungsprojekts in Kooperation mit der Siemens AG entstanden.