Internet Standards zum Policy-based Network Management

Beitrag zur IIR Konferenz „Anspruch und Realität von
Policy-based Netzwerken und Quality of Service-Konzepten“

Jürgen Schönwälder

Institut für Betriebssysteme und Rechnerverbund
Technische Universität Braunschweig
Bültenweg 74/75
38106 Braunschweig

Tel: +49 531 391 3289
Email: schoenw@ibr.cs.tu-bs.de
Web: http://www.ibr.cs.tu-bs.de/~schoenw/

Relevante IETF Arbeitsgruppen

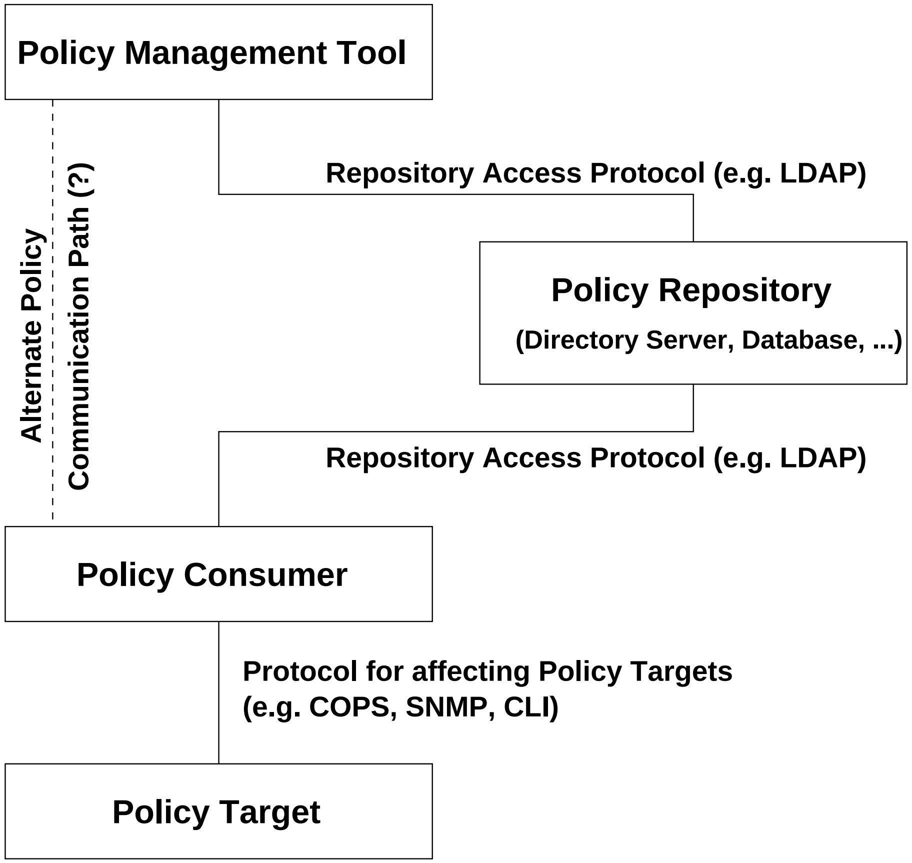
- Policy Framework (policy)
  - Terminologie für Policy-based Network Management
  - Anforderungen an Policy-based Network Management
  - Abbildung des DMTF CIM Policy-Informationsmodells in ein LDAP Datenmodell

- Resource Allocation Protocol (rap)
  - Common Open Policy Service (COPS) Protokoll
  - Policy-based Admission Control (Outsourcing Modell)
  - Policy-based Network Configuration (Provisioning Modell)

- Differentiated Services (diffserv)
  - Anwendung der Policy-Technologien auf DiffServ-Router

- Configuration Management with SNMP (snmpconf)
  - Existiert derzeit noch nicht offiziell
  - Anwendung (Erweiterung?) von SNMP zum effektiven Konfigurationsmanagement

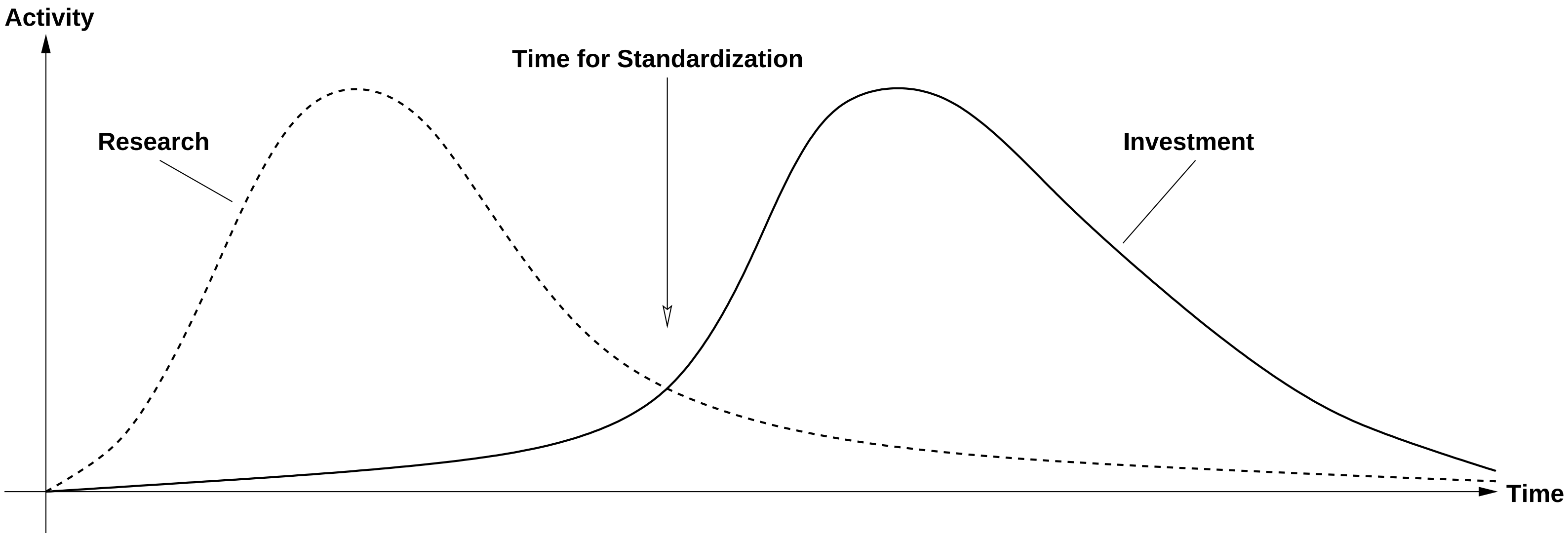
Funktionale Komponenten des Policy-Rahmenwerks



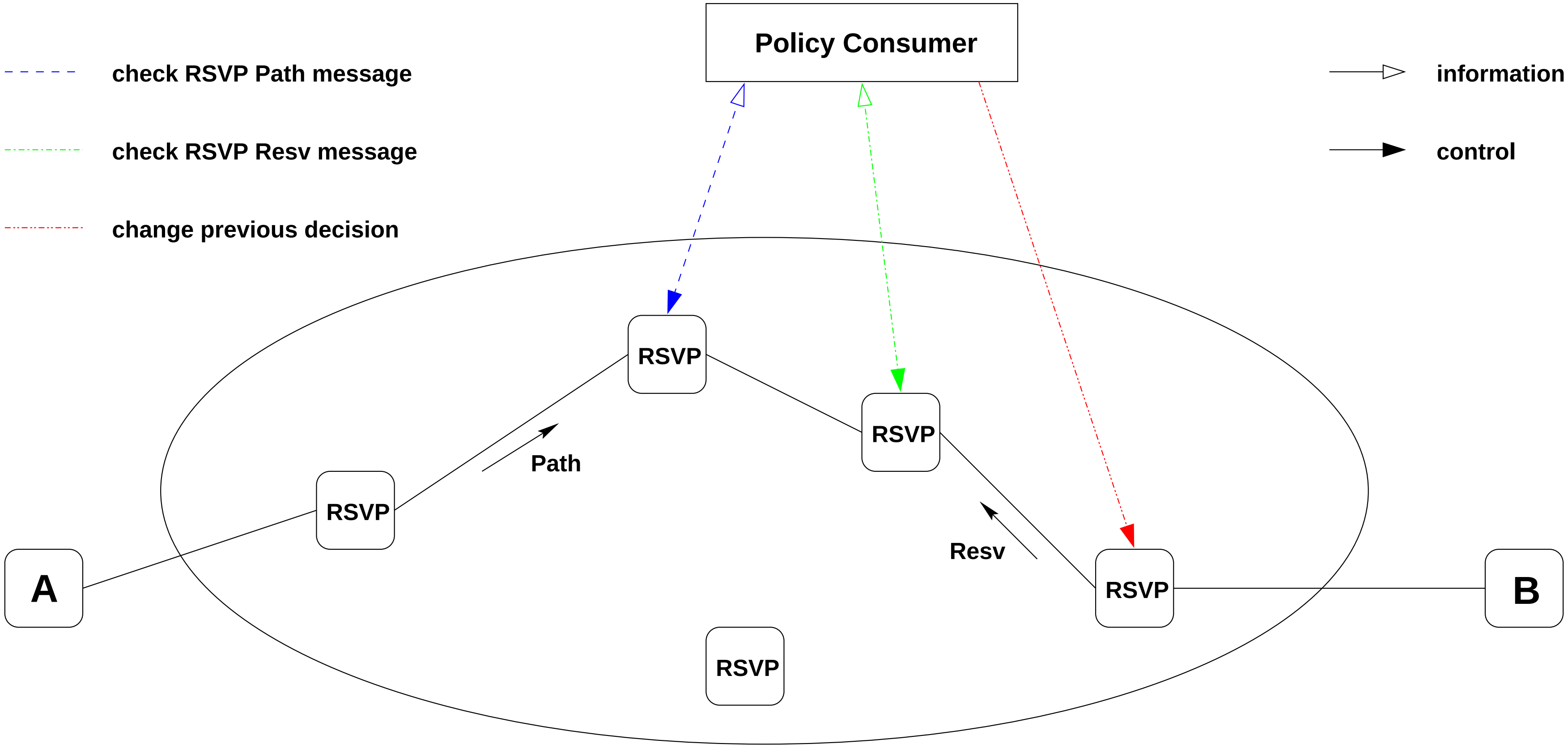
- Unvollständiges Modell:
  - Interaktionen zwischen Policy Consumern?
  - Monitoring und Status Information?
  - Informationen über die Netzwerk-Topologie?
- LDAP nur bedingt geeignet:
  - Benachrichtigungen über Änderungen?
  - Eignung zur Verteilung dynamischer Daten?
  - Versionierung von Daten?

Wo und wann sollten Standards geschaffen werden?

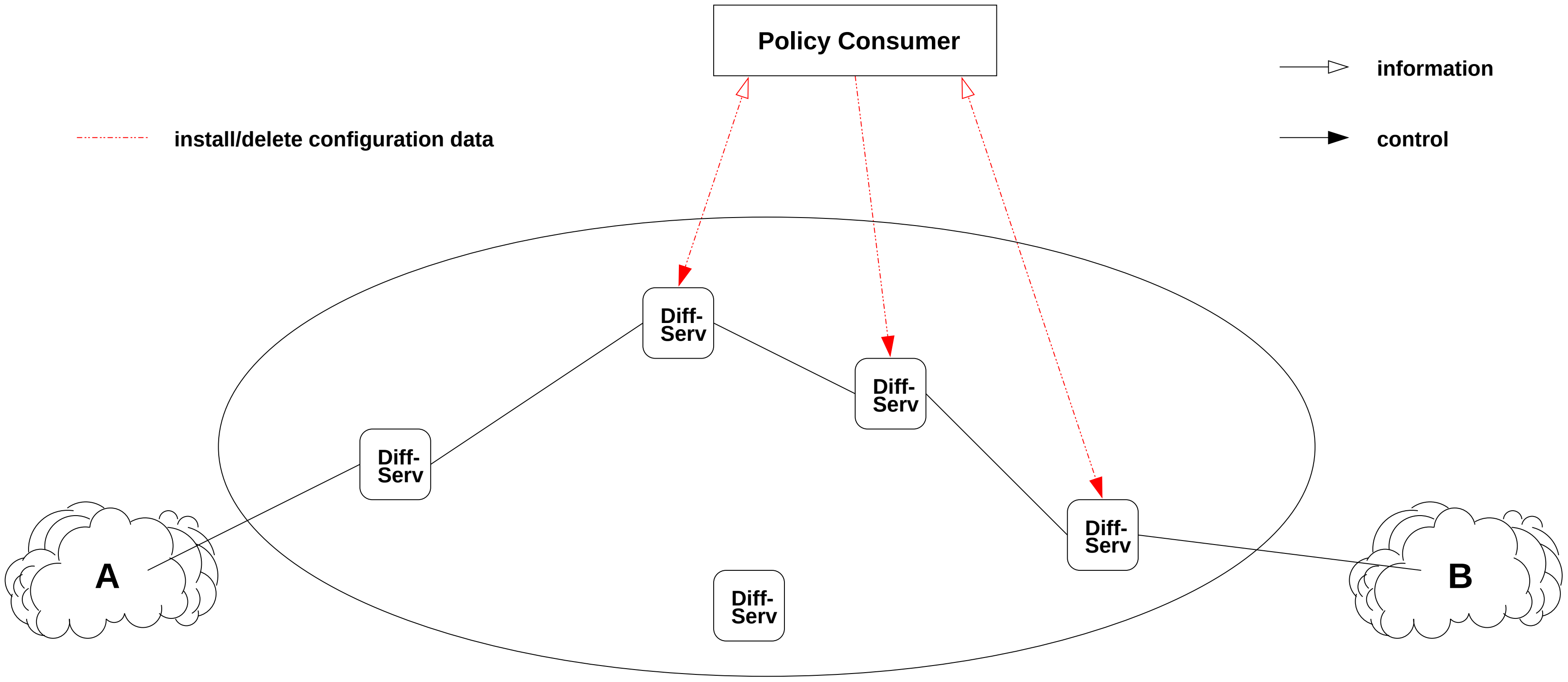
- Standards sind nur sinnvoll, wenn sie allgemein akzeptiert und implementiert werden.
- Standards müssen Herstellern Raum lassen, um ihre Produkte zu differenzieren.
- Standards können durch gemeinsame Schnittstellen neue Märkte schaffen.
- Beachte die „Theory of Standardization“ (David Clark, MIT):



Outsourcing Modell (Beispiel RSVP)



Provisioning Modell (Beispiel DiffServ)



Outsourcing versus Provisioning

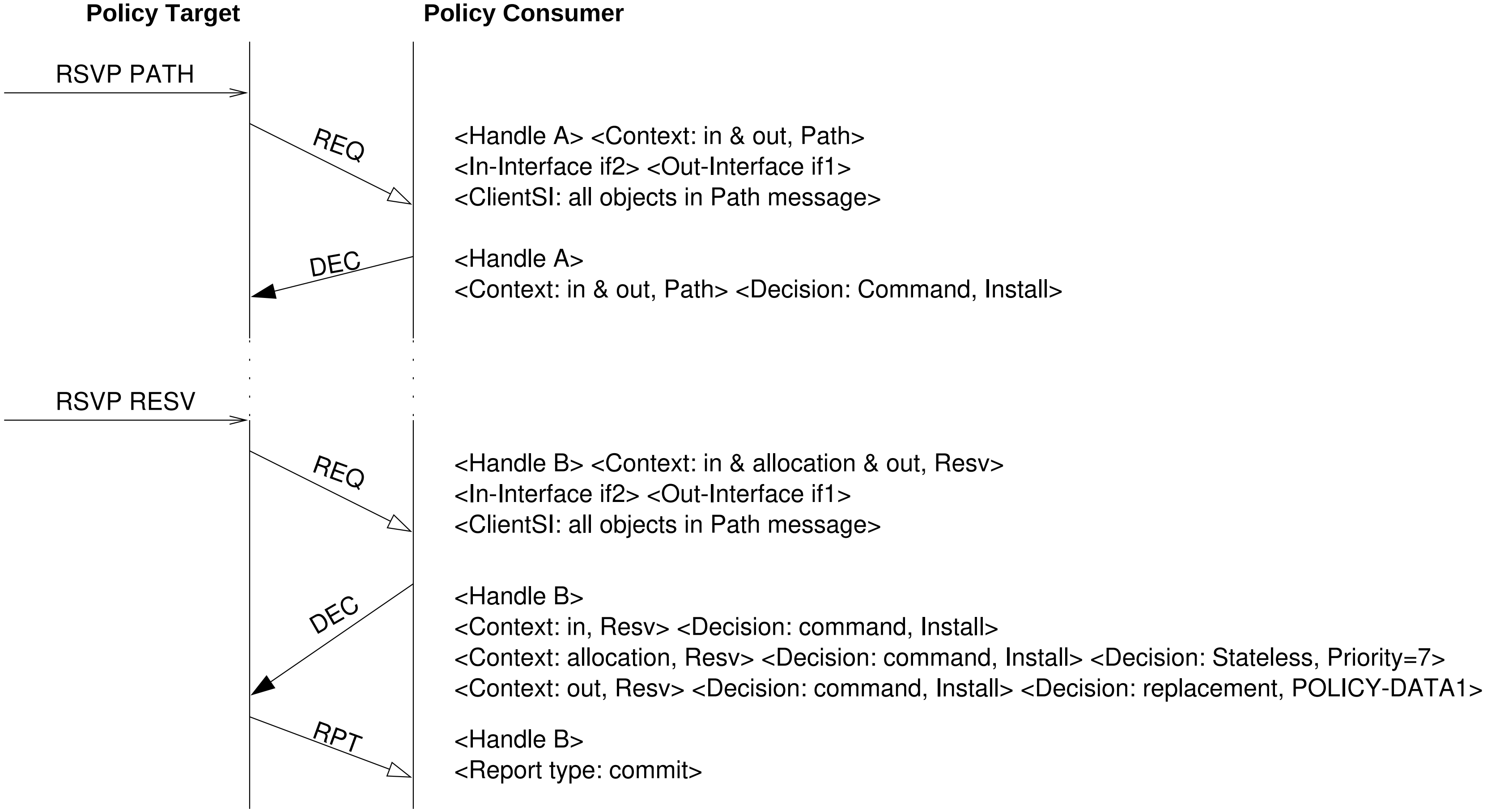
- Outsourcing Modell:
  - Entscheidungen erfolgen ereignisgesteuert während der Signalisierungphase
  - Zusätzlich asynchrone Entscheidungen vom Policy-based Managementsystem
  - Potentielles Problem: Skalierbarkeit
- Provisioning Modell:
  - Konfiguration von relevanten Informationen zur lokalen Entscheidungsfindung
  - Konfigurationsdatenmodell wird in der Policy Information Base (PIB) definiert
  - Keine Policy-Interaktionen in Realzeit
  - Hohe Skalierbarkeit

COPS Protokollübersicht

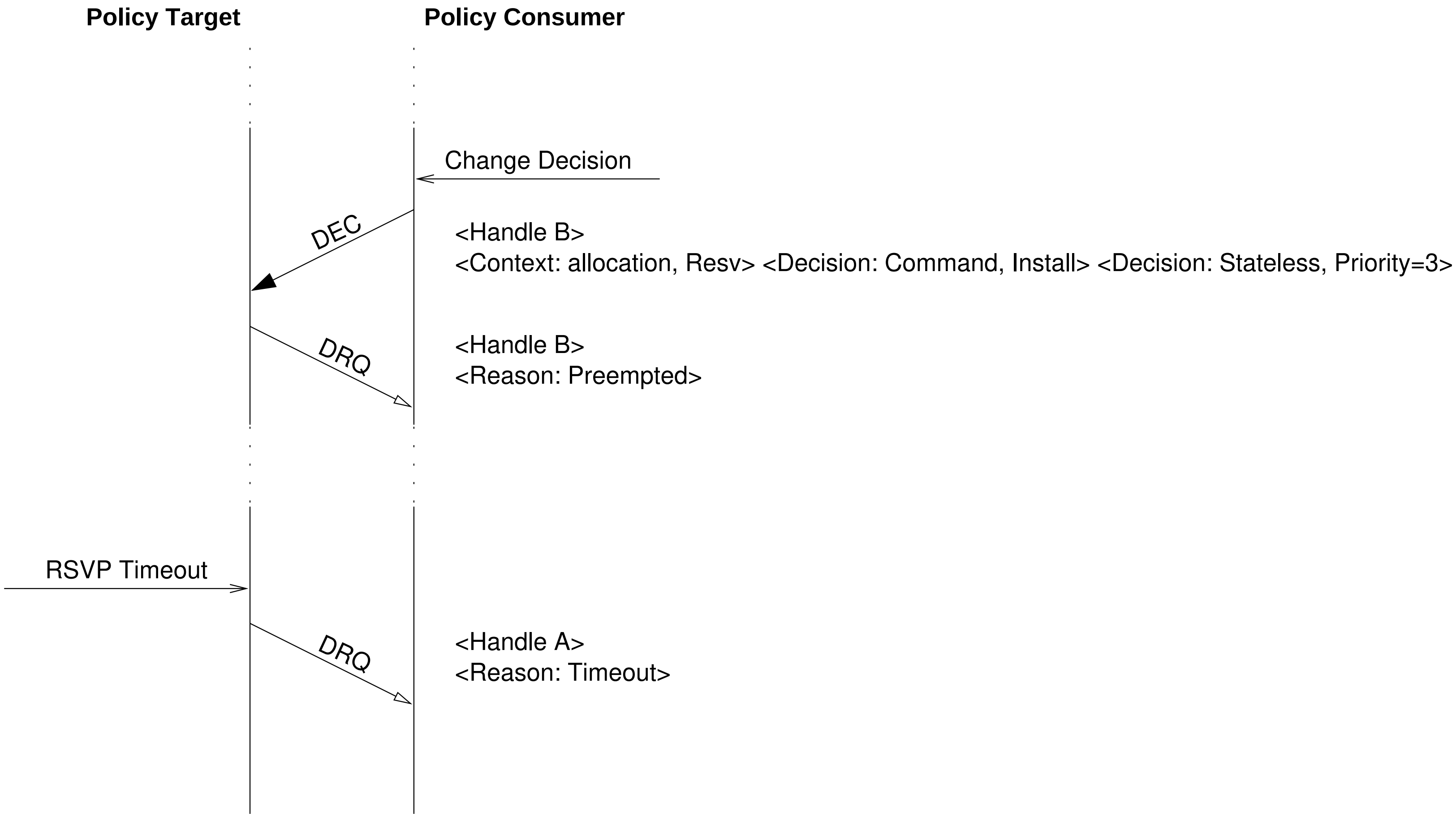
- Client/Server-Protokoll zwischen Policy Target (PT) und Policy Consumer (PC)
- Transport der COPS-Nachrichten über zuverlässiges TCP (Port 3288)
- Nachrichten enthalten eine Sequenz von erweiterbaren COPS Objekten
- Client und Server teilen sich Zustandsinformationen
- Einfache Authentifikation und Integrität durch COPS Integrity Objekte
- Benutzung von IPsec oder TLS (SSL) für weitergehende Sicherheitsdienste
- Nachrichtentypen:

REQ	Request	PT $\rightarrow$ PC
DEC	Decision	PC $\rightarrow$ PT
RPT	Report State	PT $\rightarrow$ PC
DRQ	Delete Request State	PT $\rightarrow$ PC
SSQ	Synchronize State Request	PC $\rightarrow$ PT
SSC	Synchronize State Complete	PT $\rightarrow$ PC
OPN	Client-Open	PT $\rightarrow$ PC
CAT	Client-Accept	PC $\rightarrow$ PT
CC	Client-Close	PT $\rightarrow$ PC, PC $\rightarrow$ PT
KA	Keep-Alive	PT $\rightarrow$ PC, PC $\rightarrow$ PT

COPS-RSVP Protokoll (Outsourcing)



COPS-RSVP Protokoll (Outsourcing)



Policy Information Base (Provisioning)

- Policy Information Bases (PIBs) enhalten Policy-Regeln für ein Gerät, die lokal interpretiert und angewendet werden.

- Basiert auf der SMIv2 zur Definition von SNMP MIBs.

- Bezeichnungen:

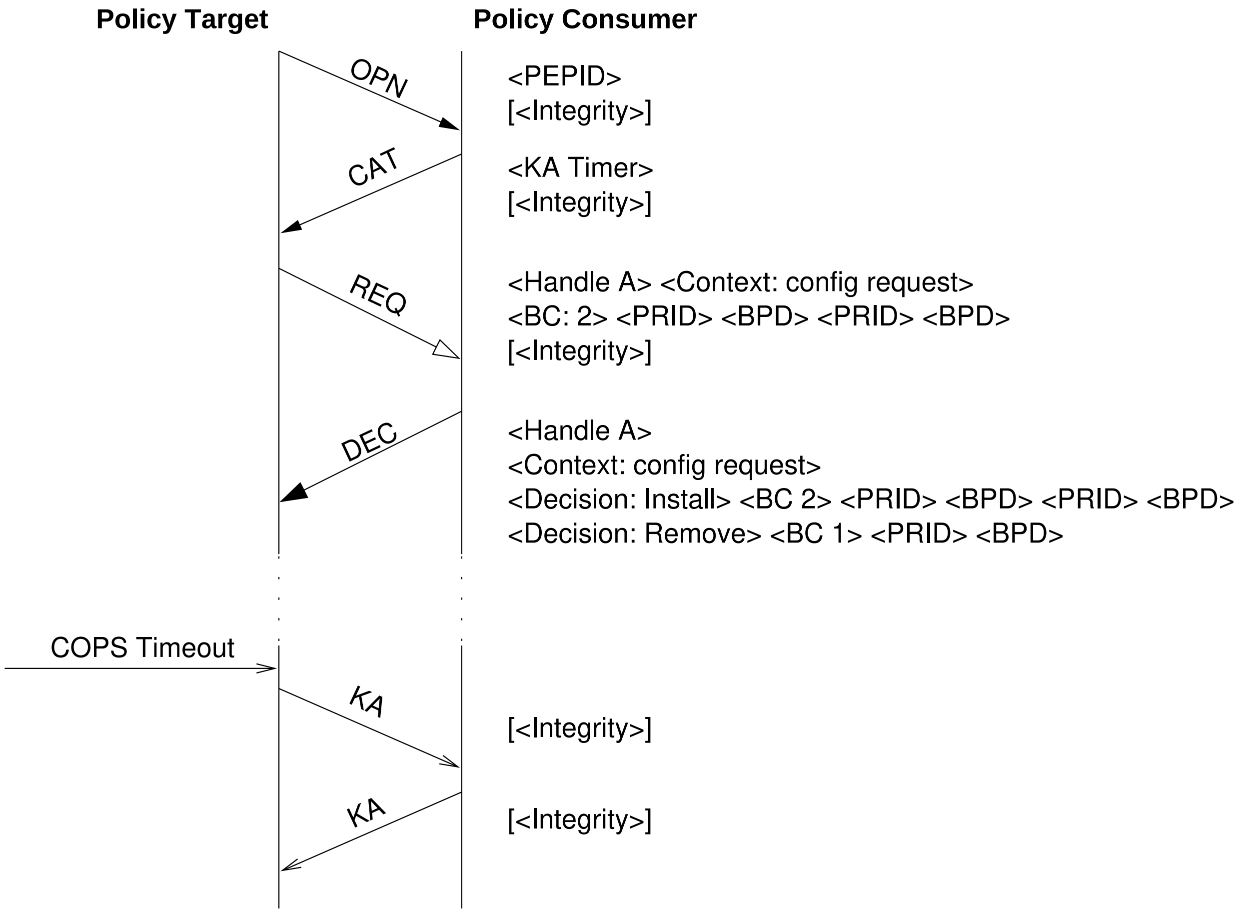
  1. Policy Rule Class (PRC)
     Identifiziert eine Regelklasse ($\rightarrow$ Zeile einer MIB Tabelle)

  2. Policy Rule Instance (PRI)
     Identifiziert eine Instanz einer Regelklasse ($\rightarrow$ Index einer MIB Tabellenzeile)

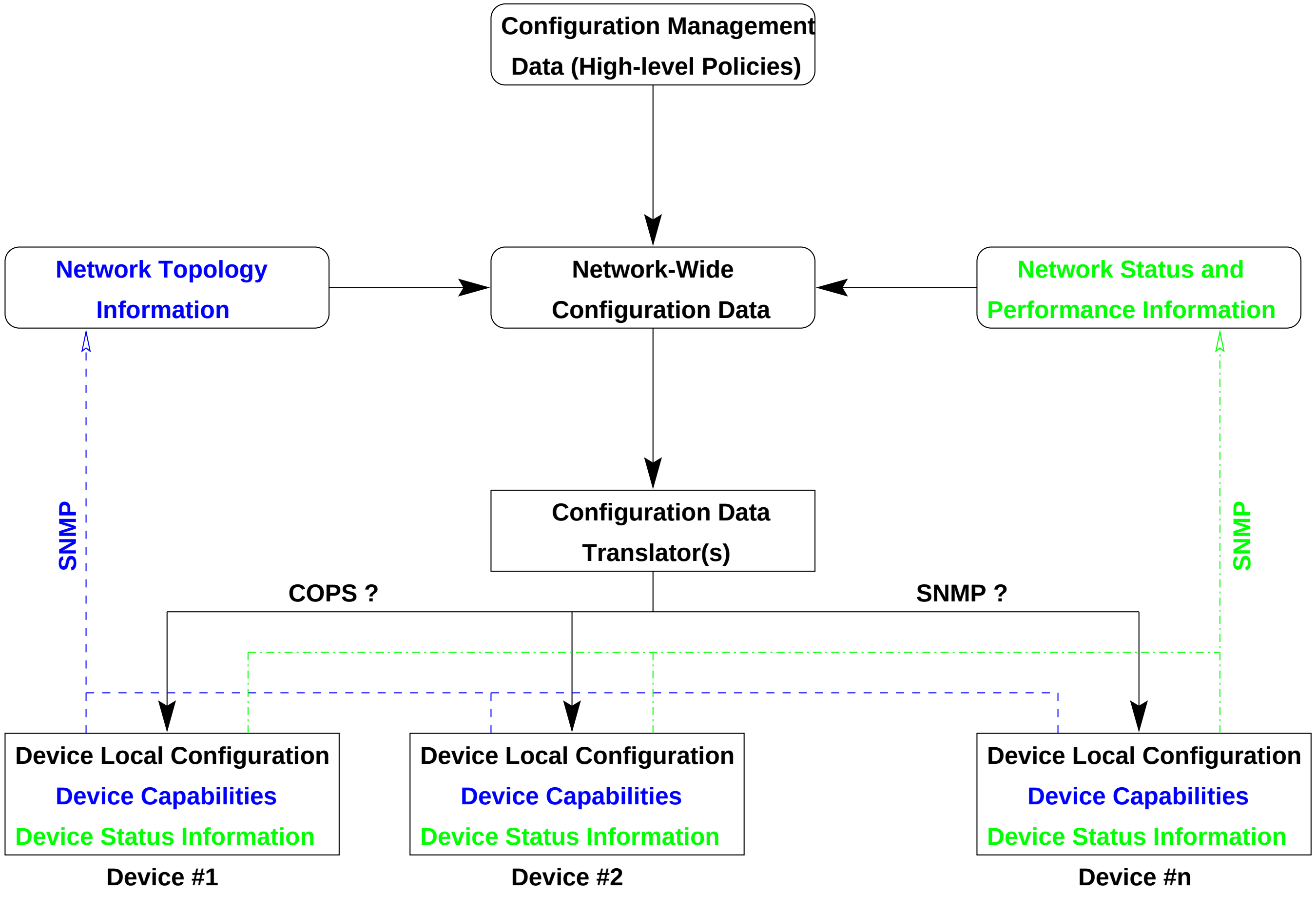
  3. Policy Rule Instance Identifier (PRID)
     Identifiziert eindeutig eine Instanz einer Regelklasse

  4. BER Encoded Policy Instance Data (BPD)
     BER kodierte Darstellung einer Instanz einer Regelklasse

COPS-PR Protokoll (Provisioning)



Policy-based Management als Konfigurationsmanagement



PIBs versus MIBs

- Policy Information Bases (PIBs):
  - Basiert auf der SMIv2 und erbt damit die bekannten Probleme der SMIv2.
  - Reduziert auf Tabellen (keine Skalare) die als Rule Classes bezeichnet werden.
  - Definition von Operationen zum Erzeugen und Löschen von Tabellenzeilen.
  - Keine vollständige Sprachdefinition vorhanden.
- Management Information Bases (MIBs):
  - Bereits ein etablierter Internet Standard (STD 58).
  - Werkzeuge und Regelsätze zur Evolution von MIB Modulen vorhanden.
  - Keine expliziten Operationen zur Erzeugung von Tabellenzeilen.
  - Mehrere Manager können gleichzeitig schreibenden Zugriff haben (Komplexität).

COPS versus SNMP

- Common Open Policy Service (COPS):
  - Zuverlässiger, effizienter Transport über TCP (große Nachrichten).
  - Granularität von Regelinstanzen (Tabellenzeilen).
  - Operationen zum Erzeugen bzw. Löschen von Regelinstanzen.
  - Gute Effizienz durch eine kompaktere Kodierung der Regelinstanzen.
- Simple Network Management Protocol (SNMP):
  - Unzuverlässiger Transport über UDP (kleine Nachrichten).
  - Granularität von einzelnen Variablen (Zellen einer Tabelle).
  - Komplexer Mechanismums zum Erzeugen bzw. Löschen von Tabellenzeilen.
  - Geringe Effizienz durch die wiederholte Kodierung von Objektnamen.

Informationsquellen

1. R. Yavatkar, D. Pendarakis, R. Guerin: *A Framework for Policy-based Admission Control*, work in progress, April 1999.

2. J. Boyle, R. Cohen, D. Durham, S. Herzog, S. Rajan, A. Sastry: *The COPS (Common Open Policy Service) Protocol*, work in progress, November 1999.

3. S. Herzog: *RSVP Extensions for Policy Control*, work in progress, April 1999.

4. J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry: *COPS usage for RSVP*, work in progress, June 1999.

5. F. Reichmeyer, S. Herzog, K. Chan, J. Seligson, D. Durham, R. Yavatkar, S. Gai, K. McCloghrie, A. Smith: *COPS Usage for Policy Provisioning*, work in progress, October 1999.

6. M. Fine, K. McCloghrie, K. Seligson, K. Chan, S. Hahn, A. Smith: *Quality of Service Policy Information Base*, work in progress, October 1999.

7. K. McCloghrie, D. Perkins, J. Schönwälder, J. Case, M. Rose, S. Waldbusser: *Structure of Management Information Version 2 (SMIv2)*, STD 58, RFC 2578, April 1999.

8. J. Saperia, J. Schönwälder: *Policy-Based Enhancements to the SNMP Framework*, work in progress, September 1999.

9. K. McCloghrie, M. Fine: *A Comparison of Policy Provisioning Protocols*, work in progress, September 1999.

10. L. Sanches, K. McCloghrie, J. Saperia: *Evaluation of COPS/PIB and SNMP/MIB approaches for configuration management of IP-based networks*, work in progress, October 1999.