Interaktive Analyse von Routing-Daten zum Schutz des Internet-Backbones
BGP-Importer, HTTP-Middleware und Web-Applikation für VAST

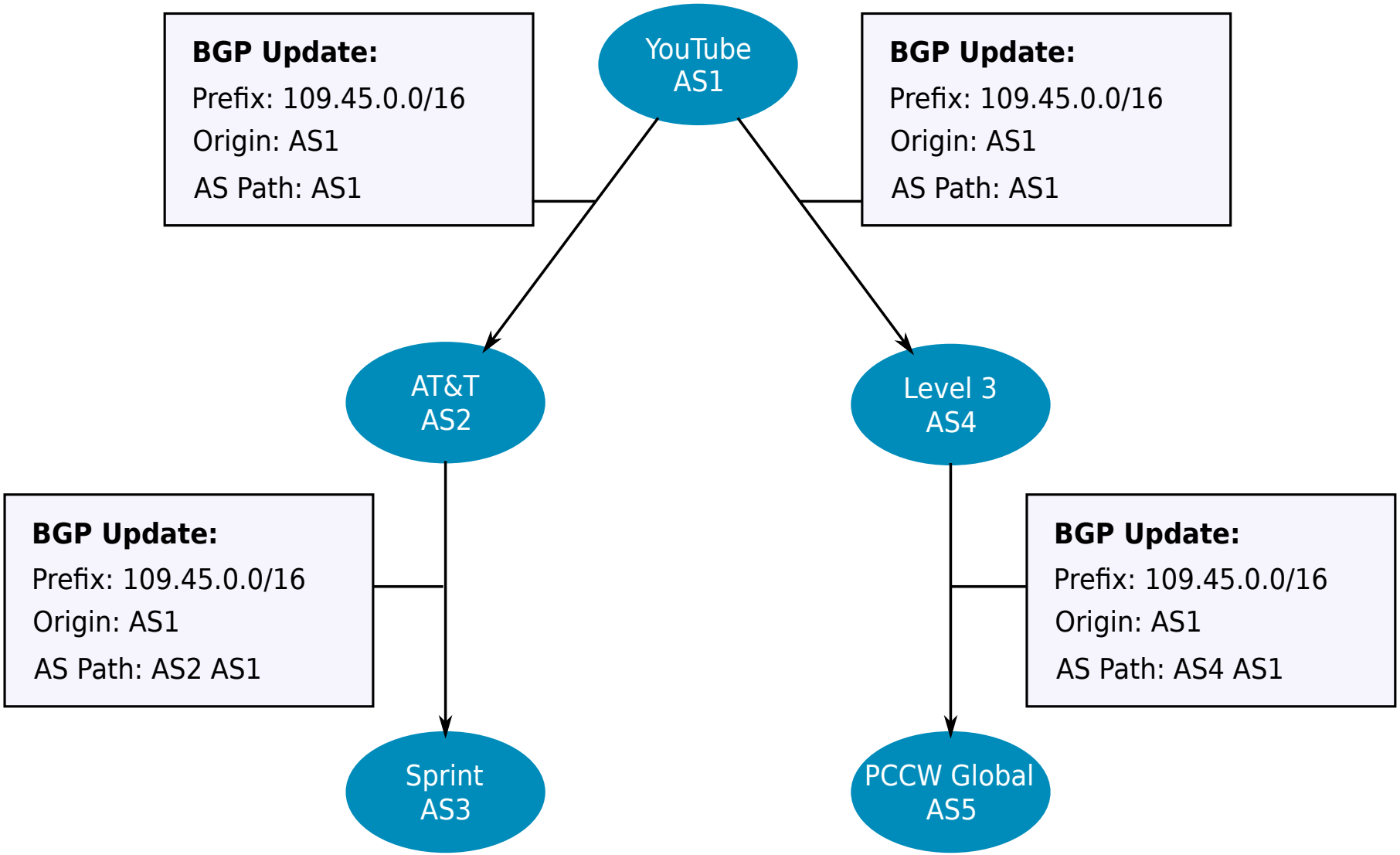
Samir Al-Sheikh, Andreas Reuter, Fabrice Ryba, Robert Schmidt
Freie Universität Berlin

Softwareprojekt Technische Informatik, SS 2015

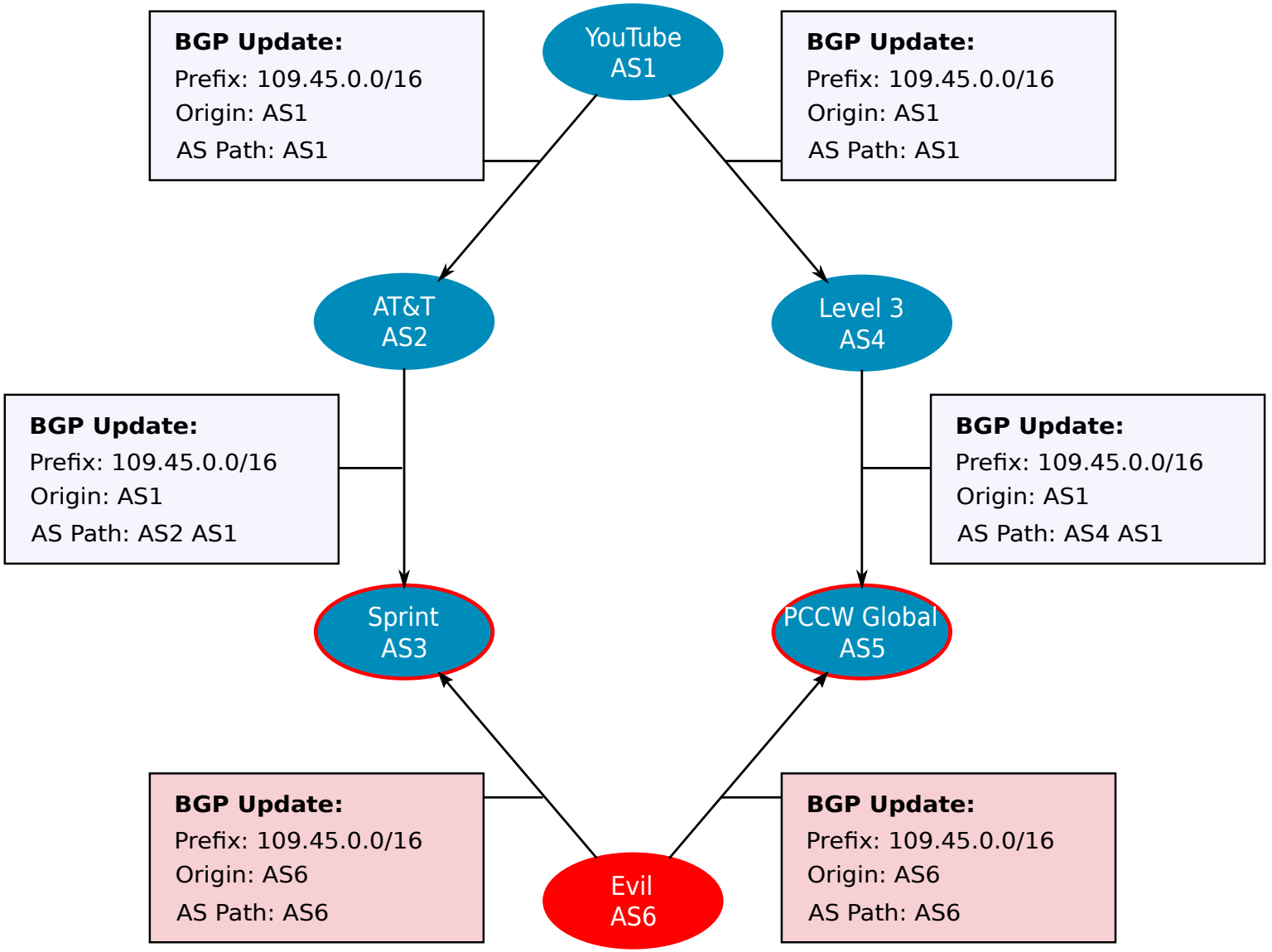
Gliederung

Gliederung

BGP Funktionsweise



BGP Hijacking



Border Gateway Protocol

- BGP ist die Grundlage für Inter-Domain-Routing

- BGP ist die Grundlage für Inter-Domain-Routing
- Liefert notwendiges Fundament für das Zustellen von IP Paketen

Border Gateway Protocol

- BGP ist die Grundlage für Inter-Domain-Routing
- Liefert notwendiges Fundament für das Zustellen von IP Paketen
- Basiert auf Vertrauen, Kooperation der teilnehmenden AS ist notwendig

Border Gateway Protocol

- BGP ist die Grundlage für Inter-Domain-Routing
- Liefert notwendiges Fundament für das Zustellen von IP Paketen
- Basiert auf Vertrauen, Kooperation der teilnehmenden AS ist notwendig
- Angriffe oder Fehler aufzuspüren erfordert Analyse von grossen Datenmengen

BGP Daten

BGP Daten

```
TIME: 06/15/15 13:40:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 193.0.0.56 AS3333
TO: 193.0.4.28 AS12654
ASPATH: 3333 1103 2603 11404 22059
NEXT_ HOP: 193.0.0.56
ANNOUNCE
  64.34.125.0/24
    76.191.107.0/24
```

BGP Daten

```
TIME: 06/15/15 13:40:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 193.0.0.56 AS3333
TO: 193.0.4.28 AS12654
ASPATH: 3333 1103 2603 11404 22059
NEXT_ HOP: 193.0.0.56
ANNOUNCE
  64.34.125.0/24
    76.191.107.0/24
```

- Route Collector rrc00: In 24 Stunden ca. 25 Millionen Updates, ca. 6.6GB Daten

VAST = Visibility Across Space and Time

Anwendungsfall: Netzwerk-Forensik

- Sehr viele Log-Dateien von verschiedenen Systemen/Protokollen
- Problem: Durchsuchen und Analysieren großer Datenmengen
- Mit herkömmlichen Mitteln sehr zeitaufwendig

VAST:

- Explorative Suchen können schnell ausgeführt werden (wichtig bei forensischen Analysen)

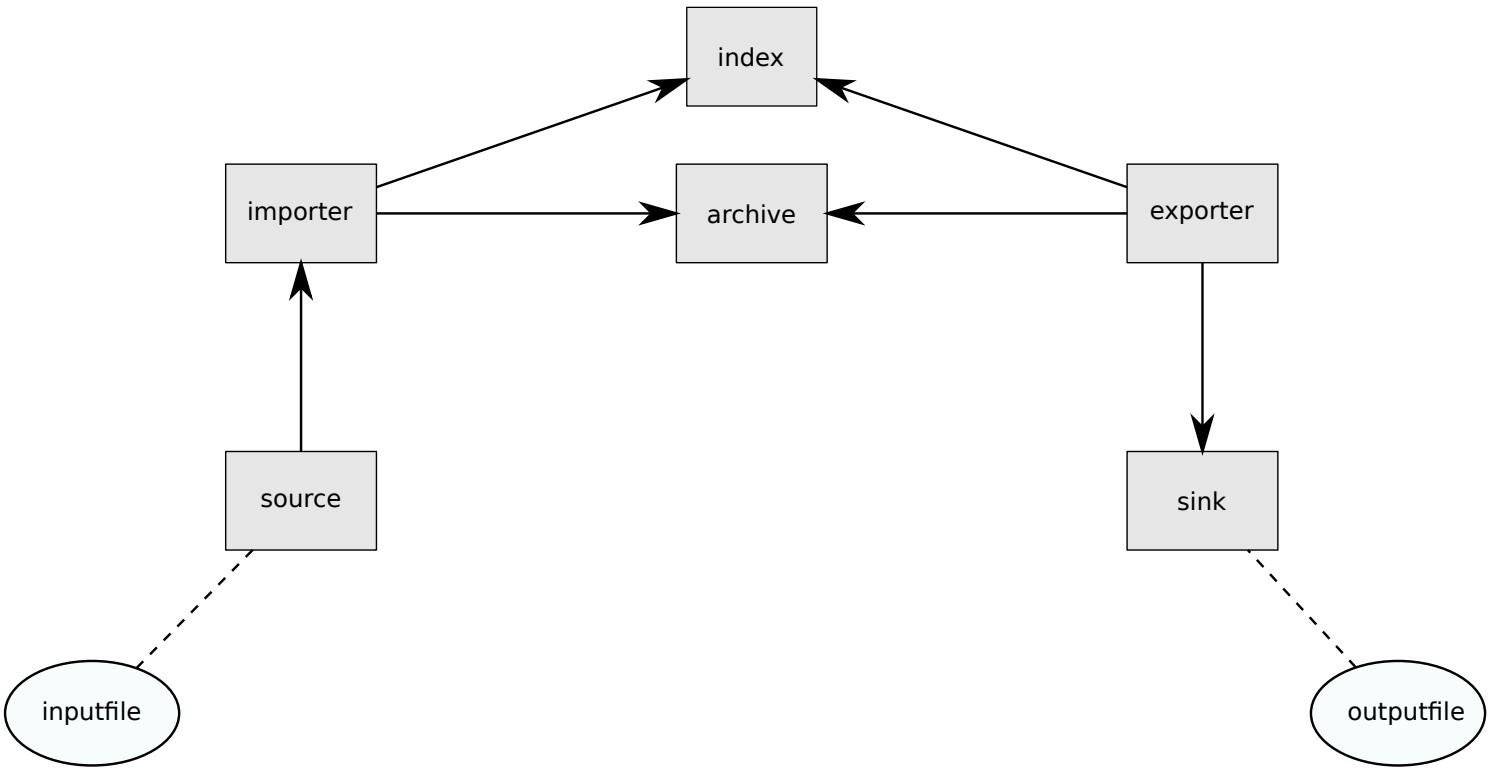
VAST:

- unterstützt Parallelität
- verteilt auf mehrere Cluster
- setzt auf das Actor-Modell auf

Actor-Modell:

- Nebenläufige Einheiten (Actor)
- Kommunikation ausschließlich über Nachrichten
- Kein gemeinsamer Speicherbereich
- Einfache Synchronisation

VAST - Architektur



Gliederung

Motivation und Ziele

Status Quo:

- BGP-Importer liest nur Text-Format ein
- nur über Konsole zugänglich

Probleme:

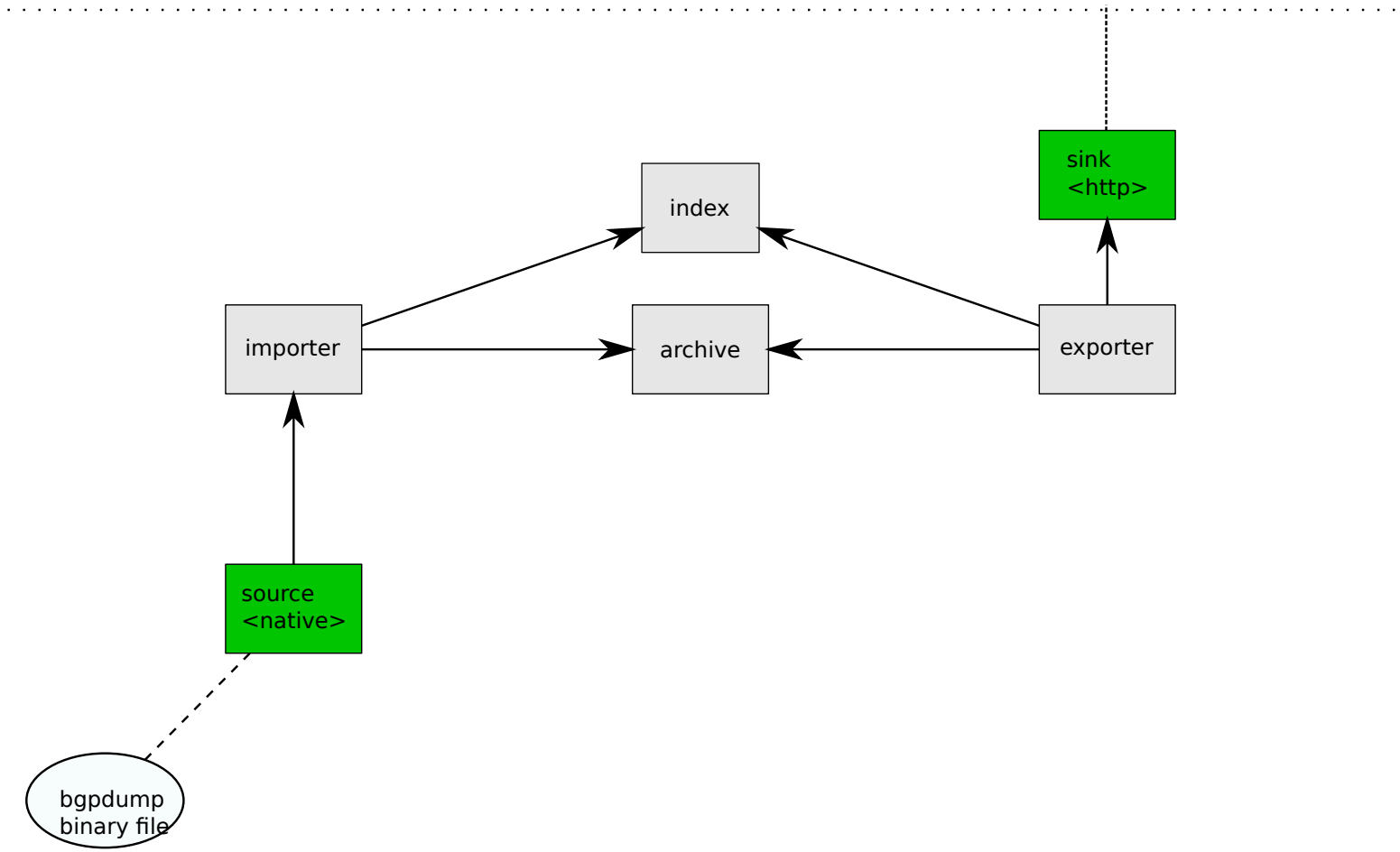
- Dateien müssen erst konvertiert werden (ineffizient)
- Keine Datenvisualisierung

Lösungsansätze:

- Erweiterung des BGP-Importers, um gängige Binär-Formate nativ einzulesen
- Erweiterung um graphische Web-Oberfläche
  - Entwicklung einer REST-Schnittstelle (Middleware)
  - Entwicklung einer Web-Anwendung für die Analyse von BGP-Daten

Gliederung

Web Interface



Importer

Importer

Ziel:

- Einlesen von BGP-Dumps

Funktionsdetails:

- Low-Order Parser interpretieren eingelesene Bytes
- High-Order Parser fassen anschließend Bytes zu Paketfeldern zusammen
- Gesamtes BGP-Paket als Event übergeben

Importer - Stand und Probleme

Heutiger Stand:

- BGP-Dumps können eingelesen werden

Probleme:

- häufige Änderungen durch aktive Entwicklung
- ungenaue Definition der Paketfelder

Nächster Schritt:

- Parallelität, um gleichzeitige Imports zu ermöglichen

Middleware

- HTTP über CAF-Nachrichten (Broker)
- Webserver als eigener Actor
- Erzeugt bei jeder Verbindung neuen Actor zur Verarbeitung und Weiterleitung der Query

Heutiger Stand:

- Query empfangen und antworten

Probleme:

- Projekt ist in aktiver Entwicklung, häufige Änderungen
- Einige Fehler

Nächster Milestone:

- Schnittstelle erweitern
- HTTP-Parser

Web-Anwendung

Motivation:

- Einfaches exploratives Durchsuchen von großen Datenmengen
  $\rightarrow$ Daten visualisieren und einfaches Filtern ermöglichen

Technologien:

- Python 3 + Django
- Kommunikation zu VAST: HTTP + JSON

Web-Anwendung - Stand und Probleme

Heutiger Stand:

- Nimmt VAST-Anfragen entgegen
- Schickt Anfrage an VAST-API
- Empfängt JSON Antwort
- Erstellt eine filterbare Tabelle

Nächster Milestone:

- Visualisieren der Routenänderungen in einem Graphen
- VAST-Anfragenerstellung durch graphische Elemente erleichtern
- Weitere Anwendungsfälle implementieren

Gliederung

Demo

...