MASTER'S THESIS

DISTRIBUTION OF LARGE DATA IN NETWORKS WITH LIMITED BANDWIDTH

WEBBASIERTE VERTEILUNG GROSSER DATENMENGEN IN LOKALEN NETZWERKEN

TIM FRIEDRICH

CHAIR

Internet Technologies and Systems

SUPERVISORS

Prof. Dr. Christoph Meinel

Dipl.-Inf. (FH). Jan Renz

October 5th, 2016

ABSTRACT

My english abstract

ZUSAMMENFASSUNG

Meine deutsche Zusammenfassung

ACKNOWLEDGMENTS

I would like to thank

CONTENTS

ACRONYMS

1

EINLEITUNG

1.1 MOTIVATION

In den letzten Jahren hat sich das verwendete Datenvolumen des Internets immer weiter gesteigert. Waren es 2015 noch monatlich 72 Petabyte pro Monat sind es 2016 bereits 96 Petabyte. Zwar ist die vorhandene Bandbreite bei vielen Nutzern ebenfalls gestiegen jedoch bezieht sich die vor allem auf Ballungsgebiete. In ländlicheren Regionen ist die Bandbreite in Deutschland in vielen Fällen weiterhin nicht ausreichend. Insbesondere wenn viele Nutzer sich gemeinsam eine Internet Anbindung teilen müssen ist dies ein Problem.*Studie*

Immer mehr Unternehmen halten Ihre Hauptversammlungen, Kundgebungen, und Pressemitteilungen über Live Streams im Internet ab.*Studie* Dies stellt sie vor das Problem das trotz oftmals guter Internetanbindung zu viele Mitarbeiter das Video über die Internetanbindung laden müssen, was zu einer volländigen Auslastung des WANs führen kann. Dies wiederum kann zur Folge haben, dass ein Arbeiten für die restliche Belegschaft schwierig bis unmöglich wird. Der dadurch entstandene Schaden ist oft nur schwer zu beziffern, geht jedoch schnell in die Millionen.(klingt ohne ref nicht gut)*Studie*

Nicht nur bei Unternehmen sondern auch in Schulen ist die Digitalisierung auf dem Vormarsch. Zunehmend werden Online-Lernplattformen im Unterricht eingesetzt. Diese Entwicklung wird jedoch stark ausgebremst durch fehlende Internet Bandbreiten. Viele Schulen haben eine schlechtere Internetanbindung als viele privat Haushalte. Um statische Inhalte anzeigen zu können, muss jeder Schüler einer Klasse sich diese über das WAN aus dem Internet herunterladen. Da jedoch Schüler in derselben Klasse oft die gleichen Inhalte benötigen, kann Bandbreite gespart werden, indem diese Inhalte nur einmal über das Internet geladen und anschließend im lokalen Netzwerk verteilt werden.

Beide Anwendungsfälle haben gemeinsam das viele Nutzer die selben Inhalte zur annähernd gleichen Zeit benötigen und zum aktuellen Zeitpunkt häufig über das Internet laden müssen. Diese Zeitliche und inhaltlich Lokalität kann genutzt werden um die benötigte Bandbreite zu reduzieren, indem die Inhalte nur einmal über das WAN geladen und anschließend im lokalen Netzwerk verteilt werden.

Die folgende Arbeit betrachtet den Anwendungsfall des Live-Streamings und den Einsatz von Unterstützender Software in Schulen. Es wird betrachtet ob ein Peer to Peer Ansatz zu einer Verbesserung von Ladezeiten und Netzwerklast betragen kann.

1.2 PROJEKT SCHUL-CLOUD

Das Projekt Schul-Cloud[1] ist ein Gemeinschaftsprojekt des Hasso-Plattner-Instituts und des nationalen Execellence-Schulnetzwerkes (MINT-EC). Im Mai 2017 startete die Pilotphase des Projektes mit insgesamt 27 Schulen. Ziel des Projektes ist die Förderung der Digitalisierung in Schulen. Zu diesem Zweck wurde eine Web basierte Plattform entwickelt die Lehrer und Schüler bei der Unterrichtsvorbereitung, Durchführung und Nachbereitung unterstützen soll.

Lehrer können Kurse anlegen und diese nutzen um Materialien sowie Aufgaben zu verteilen. Schülern ist es über die Plattform möglich Lösungen für Aufgaben einzureichen und ihr Ergebnis einzusehen. Über einen Kalender können sie Ihren Stundenplan abrufen.

Das Projekt wird als Open Source Projekt zur Verfügung gestellt und basiert auf einer Microservice Architektur. Bei diesem Architekturmuster wird die Software aus unabhängigen Softwarekomponenten(Services) zusammengesetzt. Die Komponenten kommunizieren über Schnittstellen, sind aber darüber hinaus eigenständige Entitäten und können von beliebig vielen anderen Komponenten verwendet werden. Durch die Verwendung von Microservices wird eine einfachere Anbindung an bestehende Infrastrukturen ermöglicht. Des weiteren können einzelne Services ersetzt werden um die Plattform an die Anforderungen der Schulen anzupassen. Bereitgestellt wird die Plattform mit Hilfe von Cloud Hosting Ansätzen, bei dem die Infrastruktur zentral und nicht von jeder Schule bereitgestellt wird. Dies ermöglicht eine einfache Skalierung. Neben der Web Anwendung existieren native Apps für Android und IOS.

unsicher wie detailiert ich hier werden soll

1.3 SLIDESYNC

Slidesync ist eine Live Streaming Plattform des Unternehmens Media Event Services. Sie ermöglicht es Live-Streams eigenständig anzulegen und an eine Vielzahl von Nutzern zu verteilen. Die Zielgruppe der Plattform sind mittelständische bis große Unternehmen. Neben dem Self-Service wird auch ein Managed Service Angeboten bei dem Media Event Services das komplette Streaming übernimmt. Die Plattform ist für eine große Anzahl von Nutzern ausgelegt und ist hochverfügbar um den Ansprüchen von Unternehmen gerecht zu werden. Sie

1 https://schul-cloud.org/

stellt unter anderem Funktionen bereit um Events mit Registrierung und Foliensätzen zu realisieren.

1.4 ZIELE

1.4.1 *Forschungsfrage*

- Wie können in einem Netzwerk mit geringerer Internetanbindung Datenintensiven Resourcen ausgeliefert werden?
- Eignet sich ein Peer to Peer Ansatz um die benötigte Internetbandbreite von Schulen und Unternehmen im Rahmen von Livestreams zu verbessern?

Diese Arbeit wird versuchen die Frage: Wie können in einem Netzwerk mit geringerer Internetanbindung Datenintensiven Resourcen ausgeliefert werden? zu beantworten.

Dabei wird ein Fokus auf Peer To Peer Technologien gesetzt. Zur Evaluation wird neben simulierten Benchmarks auch der Einsatz unter realen Bedingung getestet.

1.5

Hier muss klar sein was gemacht werden soll !!!

2

ABGRENZUNG

2.1 ANNAHMEN

2.2 TECHNOLOGISCHE ABGRENZUNG

- mehrere nutzer die gleiche ressourcen abrufen - Browserbasiertes P2P CDN -

3

GRUNDLAGEN

3.1 RESSOURCEN

3.1.1 *Statische Ressourcen*

Statische Ressourcen sind Inhalte einer Website die für alle Nutzer gleich sind. Sie sind im Gegensatz zu dynamischen Inhalten nicht nutzerspezifisch und können daher gut über ein CDN verteilt werden. Insbesondere die so genannten Assets einer Internetseite sind meist statisch. Dies sind meist Javascript, CSS aber auch Bild Dateien. Auch Videos fallen häufig in diese Kategorie.

3.1.2 *Dynamisch generierte Ressourcen*

Dynamisch generierte Ressourcen werden zur läufzeit der Website erzeugt und werden nicht im Vorfeld festgelegt. Dabei lässt sich zwischen Nutzergenerierten Inhalten und automatisch generierten Inhalten, z.b. Statistiken, unterscheiden.

Dynamische Inhalte sowohl Nutzer spezifisch sein, in diesem Fall werden jedem Nutzer bei selber abfrage andere Inhalte angezeigt.

3.2 CDN

Detailierter komponenten Beschreiben plus grafik. Siehe CDN Paper

Unter einem CDN, auch Content Delivery Network versteht man ein Netzwerk in dem sich Clients Inhalte von einer Reihe von Knoten laden. Ein CDN stellt dem Nutzer Auslieferungs und Speicherkapazitäten zur Verfügung. Dadurch kann die Last auf dem Ursprungsserver und die Latenz auf Seiten der Nutzer reduziert werden. Die reduzierten Ladezeiten werden unter anderem durch eine bessere geographische Nähe und damit geringerer Netzlaufzeiten erreicht.

Es lassen sich drei Klassen von CDNs unterscheiden. Infrastuktur basierte CDN die auf einer geografisch verteilten Server Infrastruktur basieren, Peer To Peer basierte CDNs bei denen die Inhalte direkt zwischen den Teilnehmern verteilt werden und Hybride CDNs die aus einer Kombination aus Server Infrastruktur und Peer To Peer Verteilung beruhen.

3.2.1 *Infrastruktur basierte CDNs*

Infrastruktur basierte CDNs bestehen aus einem Ursprungsservern, der von dem Bereitsteller der Inhalte kontrolliert wird, und einem Netzwerk aus replica Servern. Die replica Server übernehmen die Verteilung der Inhalte an die Clients. Sie fungieren als ein möglichst regionaler cache in dem Inhalte des Ursprungsservers gespiegelt werden. Ein Distributionssystem ist dafür verantwortlich die Inhalte auf den replicas zu aktuallisieren und übernimmt das Routing bei einer Anfrage eines Clients. Unter Zuhilfenahme verschiedener Metriken versucht das Distributionssystem einen möglichst optimalen replica Server für den Client zu finden. Diese Metriken unterscheiden sich zwischen den Anbietern. Häufig werden jedoch geographische Entfernung, Latenzzeiten und die Übertragungsrate berücksichtigt. Um eine möglichst geringe Latenz zu erreichen sind infrastruktur basierte CDNs häufig geografisch sehr verteilt und bestehen aus meherern tausend replica Servern. So hat Akamai, einer der größten CDN Anbietern, über 137000 Server in 87 Ländern. **[akamaiPeer]**

3.2.2 *Peer To Peer basierte CDNs*

3.2.3 *Hyrid CDNs*

Hybrid CDNs kombinieren Peer To Peer CDNs und Infrastuktur basierte CDNs. Bei hybriden CDNs wird zuerst versucht die Resource über das Peer Netzwerk zu laden. Ist dies nicht möglich wird auf ein Infrastruktur basiertes CDN zurück gegriffen. Dadurch kann die Last auf dem CDN verringert und durch die Kombination verschiedener CDNs eine bessere Ausfallsicherheit erreicht werden. Häufig kommt diese Art der CDNs zum Einsatz wenn Ressourcen für Websites mit einem Peer To Peer Ansatz verteilt werden sollen. Da in diesem Kontext nicht alle Teilnehmer die technischen Vorraussetzungen mitbringen um an dem Peer To Peer Netzwerk teilzunehmen ist eine entsprechende alternative Lösung nötig. Da die viele Websites bereits mit einem Infrastruktur basierten CDN arbeiten ist es naheliegend dieses weiter zu verwenden.

3.3 VERTEILTE HASHTABELLEN

3.4 PEER TO PEER NETZWERKE

Bei einem Peer To Peer Netzwerk handelt es sich um eine Netzwerk Struktur bei der alle Teilnehmer gleichberechtigt sind. Sie bildet damit das gegen Konzept zur klassischen Client-Server Struktur, bei der einer oder mehrere Server einen Dienst anbieten der von Clients genutzt werden kann. In einem Peer To Peer Netzwerk können die

Teilnehmer sowohl Dienste anbieten als auch nutzen. Typische wenn auch nicht notwendige Charakteristika sind laut Steinmetz[**p2pBook2005**]:

- Heteorogenität der Internetbandbreite der Teilnehmer
- Verfügbarkeit und Qualität der Verbindung zwischen Teilnehmern kann nicht vorausgesetzt werden
- Dienste werden von den Teilnehmern angeboten und genutzt
- Die Teilnehmer bilden ein Netz das auf ein bestehendes Netz aufgesetzt wird(Overlay Netzwerk) und stellen Suchfunktionen bereit
- Es besteht eine Autonomie der Teilnehmer bei der Bereitstellung von Ressourcen
- Das System ist selbstorganisiert
- Die restlichen Systeme müssen nicht skaliert werden und bleiben intakt

Sie lassen sich einteilen in zentralisierte, reine und hybride Peer To Peer Netzwerke. Zentralisierte Netze haben zur Verwaltung einen Server der unter anderem die Verbindung der Teilnehmer übernimmt. Dadurch ist es möglich eine Verbindung aufzubauen ohne das die IP Adresse im Vorfeld bekannt ist. Reine Peer To Peer Netzwerke haben keinen zentralen Verwaltungsserver. Die Verwaltung des Netzwerkes wird von den Teilnehmern selber übernommen. Das hat zur Folge das eine Verbindung nur möglich ist, wenn die IP Adresse des anderen Teilnehmers bekannt ist.

Man unterscheidet zwischen unstrukturierten und strukturierten Peer To Peer Netzwerken.

3.4.1 *Unstrukturierte Peer To Peer Netzwerke*

In unstrukturierten Peer To Peer Netzwerken wird keine Zuordnung von Objekten zu Teilnehmern gespeichert. Um ein Objekt zu finden müssen alle Teilnehmer des Netzwerks gefragt werden.(Flooding) Dadurch steigt die Belastung des Netzwerks mit zunehmender Peer Anzahl.

3.4.2 *Strukturierte Peer To Peer Netzwerke*

Strukturierte Peer To Peer Netzwerke haben eine Zuordnung von Objekt und Teilnehmer. Es ist also möglich gezielt nach einem Objekt zu suchen. Dies wird häufig über verteilte Hash Tabellen, über die mit einem verteilten Index gesucht werden kann, realisiert.

3.5 WEBRTC- WEB REAL-TIME COMMUNICATION

Webrtc ist ein offener Standard mit dem Echtzeit Kommunikation zwischen Browser und mobilen Anwendungen ermöglicht wird. Mit Hilfe von Webrtc ist es möglich eine Peer To Peer Verbindung aufzubauen und Daten direkt zwischen den Clients auszutauschen ohne das externe Plugins erforderlich sind. Insbesondere der Austausch von Multimedia Inhalten soll ermöglicht werden. Neben der Unterstützung für Video und Audio Inhalten gibt es jedoch auch die Möglichkeit Daten auszutauschen. Webrtc wird vom W3C[**w3Webrtc**] standarisiert und definiert eine Sammlung von APIs und Protokollen.

Aktuell wird Webrtc von Chrome, Firefox, Android und iOS unterstützt.[1] Webrtc implementiert drei APIs: MediaStream, RTCPeerConnection und RTCDataChannel die im folgenden genauer beschrieben werden.

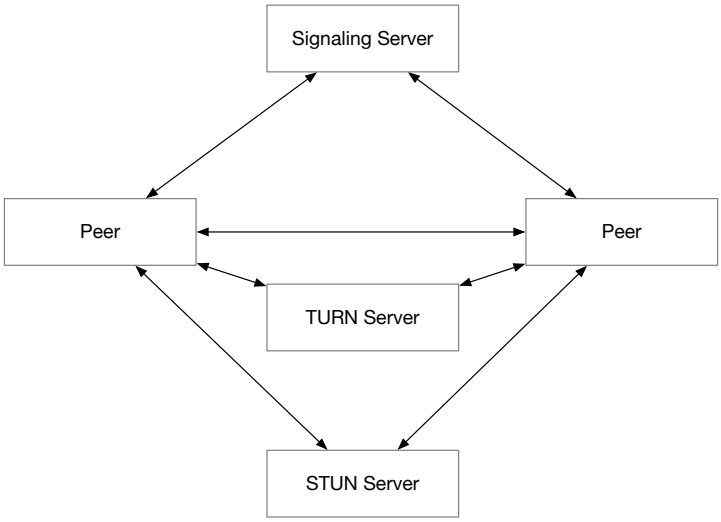

Figure 1: Überblick Server/Client Struktur Webrtc

3.5.1 *RTCPeerConnection*

- Representiert verbindung zum peer
- Code beispiel

3.5.2 *RTCDataChannel*

- Übertragung von raw data (Bitstreams)
- string, blob, arraybuffer, ArrayBufferView
- Übertragung mit Stream Control Transmission Protocol (SCTP)

1 https://caniuse.com/#feat=rtcpeerconnection

- kurze erklärung SCTP
- Verbindungsorientiertes Netzwerkprotololl
- RFC 4960
- Das zuständige Gremium bei der IETF ist die Arbeitsgruppe Signaling Transport, kurz SIGTRAN.xX
- Selbe stufe als Transportprokoll im stack wie TCP/UDP
- Konzept der Association:
- mehrere Nachrichten-Datenströme in sich reihenfolgenerhaltend
- zwischen den Datenströmen muss die Reihenfolge nicht erhalten bleiben
- Multistreaming - Ein host mehere Ips
- Vier wege Handschake
- Hierbei speichert der Server bei einer Verbindungsanfrage (INIT-Paket) keine Zustandsinformationen, sondern schickt diese in Form eines Cookies (INIT-ACK-Paket) an den Client. Der Client muss dieses Cookie in seine Antwort (COOKIE-ECHO-Paket) einfügen und wird damit vom Server als zum Verbindungsaufbau berechtigt erkannt, was dieser ihm bestätigt (COOKIE-ACK-Paket)x

3.5.3 *MediaStream*

Die Mediastream api, auch getUserMedia, ermöglicht es Echtzeit Daten wie audio oder Video aufzunehmen, anzuzeigen und an andere Clients weiter zu leiten und repräsentiert Medien Streams wie z.b. Audio oder Video Streams. Sie ermöglicht unter anderem den Zugriff auf Video Kameras und Mikrofone. Durch Sie ist es möglich auf die Hardwareunterstützung für Videos mittels open GL zuzugreifen. MediaStreams lassen sich mithilfe des src Attributes von HTML 5 video Elementen in das DOM einbinden. MediaStreams wurden von vom W3C in einem eigenen Standart definiert.[**w3MediaStream**]

3.5.4 *Singaling*

Das Signaling koordiniert die Kommunikation der Verbindungen zwischen Peers. Mit Hilfe des Signalings werden unter anderem die Metadaten ausgetauscht, die benötigt werden, um eine erfolgreiche WebRtc Verbindung aufzubauen. Unter anderem sind das:

- Session Metadaten zum öffnen/schließen von Verbindungen

- Fehler Nachrichten
- Metadaten über die zu übertragenden Medien (z.b. Codecs)
- Schlüsseldaten für verschlüsselte Verbindungen
- Netzwerk Daten wie öffentliche IP Adressen und Ports

Der Webrtc Standart legt keine für das Signaling zu verwendende Technologie und Protokolle fest um die integration mit bestehenden Technologien zu verbessern und es dem Entwicklern zu ermöglichen das für den Anwendungsfall beste Protokoll zu verwenden. Um Signaling zu ermöglichen ist ein bidirektionaler Kommunikationskanal zwischen client und server notwendig, was Websockets zu einem beliebten Kandidaten macht um das Signaling zu implementieren

3.5.5 *SDP*

- Session Description Protocol (SDP, RFC 4566)
- beschreibt eigenschaften von Eigenschaften von Multimediadatenströmen
- verwaltet kommunikationssitzungen z.b. SIP(IP-telefonie)
- keine aushandlungsmechaniken sondern nur beschreibungen der Datenströme
- v=0 o=Alice 1234 1234 IN IP4 host.provider1.com s=Video von 987654 c=IN IP4 host.provider2.com t=0 0 m=audio 20000 RTP/AVP 97 a=rtpmap:97 iLBC/8000 a=fmtp:97 mode=30 m=video 20001 RTP/AVP 31 a=rtpmap:31 H261/90000
- daten aus eigener anwendung einfügen
- Felder beschreiben? zumindest die wichtigesten/verwendeten

3.5.6 *TURN Server*

Verwaltete Netzwerke, wie die von Unternehmen, haben häufig Firewalls und Port blocking Systeme installiert um die Sicherheit des Netzwerks zu gewährleisten. Das kann dazu führen das Webrtc Verbindungen nicht aufgebaut oder daten nicht über Webrtc Verbindungen übertragen werden können.

TURN Server bieten eine Fallback Lösung für diesen Fall. Sie haben eine öffentliche IP und sind über das Internet erreichbar. Im Fehlerfall kann der Datenverkehr über einen TURN Server geleitet werden, so das die Kommunikation nicht unterbrochen wird.

3.5.7 *STUN Server - Simple Traversal of User Datagram Protocol [UDP] Through Network Address Translators*

Da die Anzahl von IPv4 Adressen begrenzt ist, verwenden die meisten Subnetze NATs. Das hat zur folge das diese Clients nicht wissen wie über welche IP Adresse und welchen Port sie erreichbar sind. Daher ist der Einsatz von STUN Servern nötig um einen Verbindungsaufbau zu ermöglichen. Stun Server überprüfen eingehende Anfragen auf IP Adresse und Port und senden diese Informationen zurück an den Client, der somit in der Lage ist diese Information weiter zureichen und damit auch außerhalb seines lokalen Netzwerkes erreichbar ist. Das STUN-Protokoll ist im RFC 3489 [**rfcStun**] definiert und ist nicht auf Webrtc beschränkt.

3.5.8 *ICE*

- Methode zur überwindung von NAT
- Interactive Connectivity Establishment
- https://tools.ietf.org/html/rfc5245
-

3.6 DATACACHE API

Die Datacache API ermöglicht es Netzwerk Requests zu cachen. Ursprünglich wurde die Api entwickelt um Serivce Workern die Möglichkeit zu geben einen Cache anzulegen und selbst zu verwalten. Dadurch ist es möglich mithilfe von Service Workern und der DataCache Api Websiten auch verfügbar zu machen wenn kein internet verfügbar ist.

- https://developers.google.com/web/fundamentals/instant-and-offline/web-storage/cache-api

3.7 INDEXEDDB

IndexedDB ist ein HTML 5 Feature um Daten im Browser zu speichern. Es wurde vom W3C standarisiert[**w3IndexedDB**] und soll den veralteten websql standard ablösen. Im gegensatz zu websql hat die IndexedDB keine strukturierte Query Language und ihr liegt kein relationelles Modell zu grunde. Sie stellt einen Key-Value Store bereit der in der Lage ist auch große Datenmengen effektiv bereit zu stellen. Dabei ist der Datenzugriff auf die selbe Domain beschränkt. Die API ist überwiegend asyncron und basiert auf Promises.

3.8 SERVICE WORKER

Service Worker sind Skripte die im Browser als separate Prozesse im Hintergrund laufen, so genannte Web Worker. Sie stellen die Funktionalitäten eines programmierbaren Netwerk Proxies bereit. Durch Service Worker ist es möglich die Anfragen einer Seite zu kontrollieren auf sie zu reagieren und in den Prozess einzugreifen.[**w3ServiceWorker**] Service Worker haben keinen Zugriff auf das DOM. Sie könne mehrere Browser-Tabs und mit Hilfe des PostMessage Protokolls können Nachrichten zwischen Service Worker und Browser-Tab ausgetauscht werden. Da Service Worker Zugriff auf den DataCache und die IndexDB haben werden sie häufig verwendet um Internetseiten offline verfügbar zu machen. Bei der Registrierung eines Service Workers wird ein URL-Scope fest gelegt für den der Service Worker zuständig ist. Nur Anfragen die sich innerhalb des URL-Scopes des Service Workers befinden können von diesem bearbeitet werden.

3.8.1 *Lebenszyklus*

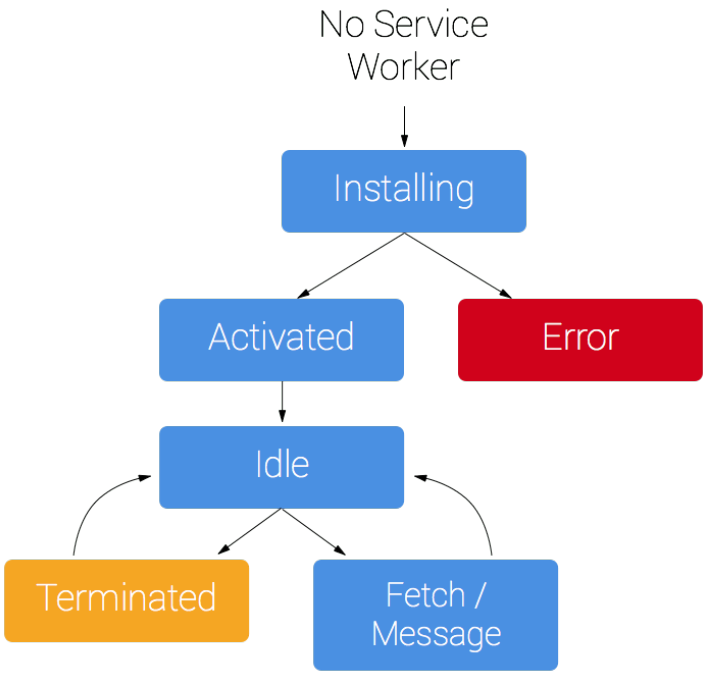

Figure 2: Lebenszyklus eines Service Workers[2]

Nach dem ein Service Worker registriert wurde befindet er sich im Zustand der Installierung. Während der Installation werden häufig Inhalte in den Cache geladen. Wurde der Service Worker erfolgreich installiert wird er aktiviert. Ab diesem Punkt kann er Requests über das fetch event abfangen. Um Arbeitsspeicher zu sparen wird der Service Worker terminiert falls er keine fetch oder message events

empfängt. Dies hat zu folge das ein Service Worker sich nicht auf den globalen Zustand verlassen kann, sondern benögten Zustand statt dessen auf die IndexedDb ausgelagert werden muss.

3.9 WEBSOCKETS

Websockets ist ein, auf TCP basierendes, Protokoll das bidirektionale Verbindungen zwischen Server und Webanwendung ermöglicht. Nachdem der Client eine Websocket Verbindung zum Server Aufgebaut hat ist es dem Server im Gegensatz zu HTTP möglich ohne vorherige Anfrage des Clients Daten an ihn zu senden. Zum initieren einer Verbindung wird ein Handshake durchgeführt der vom Client angestoßen werden muss. Dazu wird wie bei HTTP der Port 80 verwendet. Der Server antwortet bei erfolgreichem Handshake mit dem HTTP status code 101. Um eine Abwärtskompatibilität zu gewährleisten werden ähnliche Header wie bei HTTP verwendet.

Neben dem unverschlüsseltem URI-Schema ws definiert RFC6455[**rfcWebsockets**] auch das verschlüsselte Schema wss. Da sehr wenig daten overhead bei der Kommunikation besteht eigenen sich Websockets insbesondere für Anwendungen die eine geringe Latenz benötigen. Websockets werden von allen modernen Browsern unterstützt.

RFC6455[**rfcWebsockets**]

3.10 DISTRIBUTED CACHES

- Hier algorithmen erklären?
- auf hashes eingehen
- wie ein hash nur verteilt

3.11 IP ADRESSEN

Eine IP Adresse ist ein eindeutiger Identifier für Computer in einem Netzwerk. Jedem Computer in einem Netzwerk wird eine eindeutige IP Adresse zugewiesen über die der Computer adressierbar ist. Dadurch ist der Computer für andere erreichbar. Sie wird benötigt um ein routing vom Sender zum Empfänger zu ermöglichen. [**www**]

3.11.1 *Aufbau von IP Adressen*

IPv4 wurde im Jahr 1981 durch das RFC 791[**rfc791**] definiert und besteht aus einer 32 stelligen Binärzahl wodurch maximal 4.294.967.296 Adressen dargestellt werden können. Zur besseren Lesbarkeit werden IPv4 Adressen meist als vierer Blöcke in Dezimal geschrieben. IP Adressen bestehen aus einem Netz- und einem Hostanteil. Mit dem

Table 1: Beispiel einer IP Adresse mit Subntzmaske

IP-Adresse	145.574.322.	5
Subnetzmaske	255.255.255.	0
	Netzanteil	Hostanteil

Netzanteil wird das Teilnetz indem sich das Gerät befindet beschrieben, während der Hostanteil das Gerät identifiziert. Durch eine Subnetzmaske wird festgelegt welcher Teil der IP-Adresse Host- und welcher Netzanteil ist. Alle Bits die in der Subnetzmaske 1 sind legen den Netzanteil fest - alle bits die 0 sind den Hostanteil.

Aufgrund der stark ansteigenden Zahl an Geräten die mit dem Internet verbunden sind ist der Adressbereich der IPv4 Adressen nicht mehr ausreichend. Entwickelte der ITFE 1998 einen neuen standard. IPv6 verwendet 128 anstatt der 32 Bits zur Darstellung von IP Adressen. Dadurch ist es möglich 2^{32} Geräte abzubilden. IPv6 wird meist als vier Oktette in hexadezimal dargestellt. Zur Unterscheidung von Host- und Netzanteil werden Präfixlängen angegeben.

3.11.2 *Network Adress Translation(NAT)*

Mit Hilfe von NAT können mehrere Geräte über die selbe öffentliche IP-Adresse über das Internet verbunden werden. Dadurch ist es möglich trotz des begrenzten Adressraums von IPv4 mehr Geräte mit dem Internet zu verbinden. Dazu werden werden vom die IP-Adress header Felder der Datenpackete verändert.

3.12 RUBY ON RAILS

Ruby on Rails ist ein in Ruby geschriebenes Opensource Webframework. Zentraler Ansatz der Entwicklung des Frameworks ist es, es Software Entwicklern einfacher zu machen Webanwendungen zu schreiben. Die Philosopie des Frameworks beinhaltet zwei Prinzipien:[3]

Don't Repeat Yourself(DRY): Jede Information und funktionalität soll einen representation im System haben. Dardurch soll erreicht werden das die Software einfacher wartbar, übersichtichtlicher und fehlerfreier sein.

Convention over Configuration: Um die Entwicklung für den Programmierer zu erleichtern werden annahmen getroffen und standard Einstellungen festgelegt. Diese lassen sich zwar durch die Entwickler ändern sind zu beginn jedes Projektes erst einmal gleich. So werden z.b. auch Vereinbarungen über die Benennung von Methoden und Klassen getroffen(Naming Conventions).

3 https://guides.rubyonrails.org/

Ruby on Rails ist ein Model View Controller basiertes Framework.

MVC Beschreiben?

3.13 TURBOLINKS

- Javascript library
- beschleunigt navigation auf seite
- Seite wird nicht komplett geladen
- Requests werden über ajax vor dem rendern abgefangen
- nur der teil der sich geändert hat wird neu gerändert
- caching
- javascript scripte müssen nicht neu geladen werden
- https://github.com/turbolinks/turbolinks

3.14 SINGLE PAGE APPLICATIONS

Unter Single Page Applications(SPA) versteht man Webanwendungen bei denen der Client aus einem einzigen HTML Dokument besteht. Inhalte werden meist dynamisch mit AJAX oder Websocket nachgeladen. Dadurch entsteht ein Nutzererlebnis das flüssiger erscheint da Seiten nicht bei Navigation komplett neu geladen werden müssen. Sie bieten sich für Anwendungen mit hoher Nutzerzahl an da der Aufwand der HTML renderings com Server auf den Client verlagert wird. Da das Backend zumeist nur Daten ausliefert wird die Entwicklung nativer Clients für Mobilgeräte vereinfacht da zumeist das Backend wiederverwendet werden kann.

Woher quellen nehmen??? online??

3.15 REDIS

Bei Redis handelt es sich um einen In-memory Datenstruktur Speicher der als LRU cache, Datenbank oder message broker verwendet werden kann.[4] Redis ist ein Opensource Projekt und wird von Redis Labs gesponsort. Jede gespeicherte Datenstruktur ist über einen Key abrufbar.

Unter anderem unterstützt Redis folgende Datentypen: Set: Bei Sets handelt es sich um Mengen die Strings beinhalten können. Wobei jeder String nur einmal pro Set vorkommt. Hinzufügen von Element, Löschen von Elementen und das prüfen ob ein Element in einem Set vorhanden ist passieren in konstanter Zeit. (O(1))

4 https://redis.io/

Strings: Redis Strings sind binary safe, das heist sie können jegliche Daten, z.B. auch Bilddaten, enthalten. Strings können auch als atomare counter verwendet werden. Dazu stellt Redis commandos bereit zum erhöhen oder subtrahieren von Strings.

List: Listen enthalten eine geordnete Liste von Strings, in der Reihenfolge in der sie hinzugefügt wurden. Elemente können sowohl vorne als auch hinten in die Liste eingefügt werden

4

KONZEPT

4.1 NETZWERK STRUKTUREN

Anwendungsfall analyse? – evt in einleitung schieben.

Im Folgenden wird betrachtet wie die Netzwerkstruktur der Clients im Falle von Slidesync und Schul-Cloud zusammensetzen.

4.1.1 *Schul-Cloud*

Bei der Schul-Cloud lassen sich im wesentlichen zwei Hauptanwendungsszenarien unterscheiden. Zum einen die Anwendung im Unterricht. Der Lehrer stellt z.B. eine Aufgabe die mit Hilfe der Schul-Cloud durchgeführt werden soll. Daraufhin besuchen die Schüler die entsprechende Seite und bearbeiten die Aufgabe. In einem kurzen Zeitfenster laden also mehrer Schüler während sie sich im gleichen lokalen Netzwerk befinden, dem der Schule, die selben Inhalte herunter. Bei dem anderen Szenario wird die Schul-Cloud außerhalb des Unterrichts genutzt. Z.B. bereitet der Lehrer den Unterricht vor oder die Schüler bearbeiten gestellte Hausaufgaben. Die Nutzer befinden sich nicht zwangsläufig im selben Netzwerk. Auch Laden die Nutzer die selben Daten nicht notwendigerweise in einem kurz Zeitfenster sondern verteilt über einen längeren Zeitraum. Es findet jedoch auch keine so starke Auslastung des Netzwerks statt. Deshalb wird im Rahmen dieser Arbeit vor allem das erste Szenario betrachtet.

4.1.2 *Slidesync*

Die Verteilung der Clients auf Netzwerke kann sich bei Slidesync von Event zu Event stark unterscheiden. Da sich Slidesync jedoch hauptsaächlich für Streams von mittleren bis großen Unternehmen wendet, lässt sich beobachten das viele der Nutzer sich gemeinsam in einem lokalen Netzwerk, einem Standort, befinden. Um die Last der Unternehmensnetzwerke zu reduzieren, werden bei einigen Unternehmen caching Server eingesetzt. Betrachtet man 10 Events mit caching Infrastruktur im Internen netz stellt man fest das 64% der Teilnehmer aus dem internen Netz auf das Event zugegriffen haben. *caching erklären*
In dieser Arbeit wird betrachtet wie die Last auf das interne Netz re-

duziert werden kann ohne das zusätzliche caching Server eingesetzt werden müssen.

4.1.3 *Gemeinsamkeiten*

4.2 ARCHITEKTUR

Beim klassischen Client Server Modell muss sich jeder Client Ressourcen über das WAN laden. Abbildung 3 zeigt den typischen Aufbau eines solchen Netzwerks. Sind die geladenen Ressourcen groß kann die WAN Anbindung zu einem Flaschenhals werden. Durch die dadurch resultierenden langen Ladezeiten kann es zu einer starken Einschränkung des Nutzererlebnisses und der Nutzerzufriedenheit kommen.(*studie einfügen*)

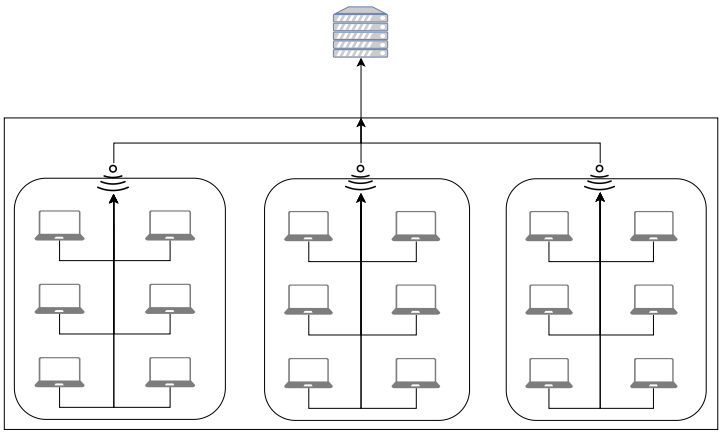

Figure 3: Netzwerkverkehr in einem herkömmlichen Netzwerk

In den betrachteten Anwendungsfällen besteht eine hohe zeitlich und inhaltliche Lokalität der Daten. Dies kann genutzt werden um die benötigte Bandbreite zu reduzieren. Dazu soll im Folgenden eine interne Verteilung mittels eines hybriden Peer To Peer CDNs untersucht werden. Abbildung 5 zeigt exemplarisch den Aufbau eines solchen Netzwerkes. Anstatt das jeder Client sich die Ressource von einem externen Server lädt, lädt nur noch ein Nutzer je Subnetz die Resource über das WAN. Dieser verteilt die Resource dann im internen Netzwerk an andere Clients die diese dann ebenfalls wieder bereitstellen.

Benötigt ein Client eine Resource versucht er zunächst die Resource über sein Peer To Peer Mesh zu laden. Ist dies nicht möglich lädt er sie über einen externen Server. Hat ein Peer eine Resource geladen speichert er sie zwischen und stellt sie für andere Clients bereit.

Da sowohl im Kontext der Schule als auch bei Unternehmen kein Wissen im Bereich der Computer Administration seitens der Nutzer vorausgesetzt werden kann, muss ein Ansatz gewählt werden der keine Installation auf Seiten der Nutzer benötigt.

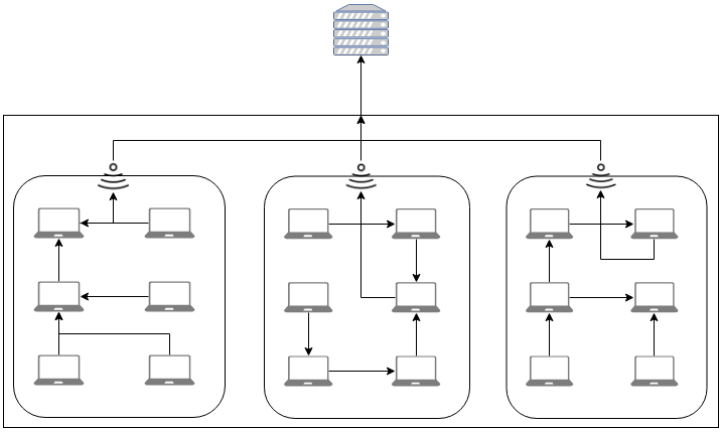

Figure 4: Netzwerkverkehr in einem Peer To Peer CDN

Um dies zu erreichen wird eine Kombination aus Webrtc und Service Workern verwendet. Der Javascript Code lässt sich als ein Plugin einbinden und erfordert nur geringen Konfigurationsaufwand seitens der Anwendungsentwickler. Da sich die Art der Seitennutzung von Anwendung zu Anwendung jedoch stark unterscheidet muss das Peer Meshing serverseitig für jede Anwendung geschrieben werden. So kann Domainenspezifisches wissen ausgenutzt werden um eine bessere überlappung der von den Clients benötigten Ressourcen zu erreichen.

Die eingesetzte Technologie zur Übertragung von Daten zwischen Browsern ist WebRTC. WebRTC ist ein offener Standard und ermöglicht es Browser paarweise zwecks Datenaustausch zu verbinden. Der große Vorteil dieser Technologie ist, dass sie direkt von modernen Browsern unterstützt wird, wodurch keine zusätzliche Software installiert werden muss. Konkret werden Webrtc DataChannel genutzt.

Für den Datenaustausch müssen wechselseitig DataChannel zueinander aufgebaut werden. Die Ausgangslage ist, dass die Peers wissen, dass es den anderen gibt, aber nicht wie der jeweils andere zu erreichen ist. Um diese Problematik zu lösen, existiert ein Vermittlungsserver (Signaling server).

Als erstes werden Informationen, über die Verbindung die aufgebaut werden soll, an den Signaling server gesendet. Es wird ein SDP-offer gesendet(SDP für Session Description Protocol). Dieses SDP-offer leitet der Signaling server an die Peers in dem selben Mesh sind weiter. Geantwortet wird mit einer SDP-answere, welche Informationen über die abgestimmte Verbindung enthält und über den Signaling server zurück geleitet wird.

Damit eine direkte Verbindung aufgebaut werden kann, müssen über den Signaling server noch weitere Informationen wie ICE-Kandidaten ausgetauscht werden. ICE steht hierbei für Interactive Conectivity Establishment und ist fester Bestandteil von WebRTC. Es ist für den Aufbau der Browser-zu-Browser-Verbindung verantwortlich. ICE-Kandidaten

enthalten hauptsächlich Informationen darüber wie ein bestimmter Nutzer erreichbar ist (also z.B. private oder öffentliche IP-Adresse). Ermittelt werden diese ICE-Kandidaten mithilfe eines STUN-Servers und dem dazugehörigen Session Traversal Utilities for NAT (STUN) Protokoll. Wie der Name des Protokolls schon verrät, wird es vor allem benötigt um auch Nutzer erreichen zu können die keine eigene öffentliche IP-Adresse besitzen, bei denen also Network address translation (NAT) eingesetzt wird. Dies ist aufgrund der mangelnden Anzahl an IPv4-Adressen bei fast jedem Internetnutzer der Fall.

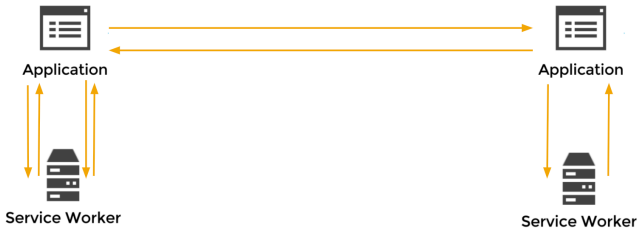

Figure 5: Service Worker - Webrtc

- Browser based without plugin
- einfache einbindung
- Server architektur diagram –> Server, Stun, CDN, P2P CDN
- Discussion verschiedener Request interception techniken
- Special Tags
- http interceptor
- only ajax calls
- erst wenn seite komplett geladen
- Browser Plugins
- evtl coporate cdn erwähnen
- extra software auf client
- Service Worker – > WEBRTC
- Script für execution

- Webrtc - Datachannel
- Service worker cached request
- warum service worker
- vergleich anderer Ansätze
- Literatur anschauen

4.3 JAVASCRIPT PROXIES - ABFANGEN VON ANFRAGE

Damit ein Client-seitiges CDN möglich ist, ist es notwendig das die Abfragen des Browsers abgefangen und auf anderem Weg beantwortet werden können. Nachdem der Browser nach einer Anfrage URL augelöst hat(DNS-lookup) lädt er die angefragte Seite. Ist die Seite geladen beginnt der Browser die im HTML Dokument verlinkten Dokumente zu laden. Das sind neben Bildern auch CSS und Javascript Dateien. Ein CDN muss in der Lage sein auf all diese Anfragen reagieren zu können.

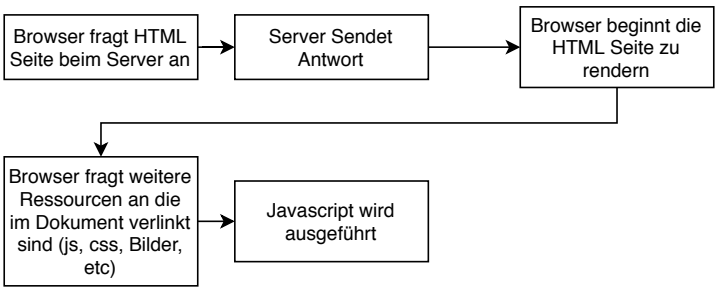

Figure 6: Ablauf einer HTML abfrage im Browser

Um dies zu realisieren gibt es verschiedene Möglichkeiten. Turbolinks unterbricht die weiterleitung nachdem ein Link angeklickt wurde und lädt die angefragte Seite mit Ajax. Dadurch ist es möglich die zu renderenden Elemente selbst auszuwählen und manuell teile der Seite zu cachen. Dieser Ansatz ließe sich auch für ein CDN verwenden. Allerdings ist es nötig die Javascript Page load Events durch eigene Events zu ersetzen und bestimmte Teile des Javascript Codes umzuschreiben. Javascript Code wird bei diesem Ansatz nach Navigation auf eine neue Seite nicht neu geladen. Auch wenn dies die Ladezeiten verringert ist eine integration ohne Anpassung des Anwendungscodes nicht möglich. Ebenfalls ist es nicht möglich Anfragen abzufangen die beim ersten Besuch der Seite entstehen, sondern nur solche die nach weiterer Navigation entstehen.

Eine weitere Möglichkeit besteht darin eigene HTML tags einzuführen und diese nachdem die eigentliche Seite und das CDN script geladen wurde mit Ajax nachzuladen. Dadurch lässt sich mit Javascript kontrollieren woher die Ressource geladen werden soll. Allerdings können Ressourcen die über das Peer To Peer CDN geladen werden

sollen erst geladen werden wenn das komplette HTML Dokument und das CDN script geladen sind. Dies kann die Ladezeiten beeinflussen und ebenfalls Anpassungen im Javascript Code der Anwendung notwendig machen. Wird in einer nachgeladenen Javascript Datei ein Eventhandler auf ein Event registriert das bereits gefeuert wurde, so wird dieser Code nicht mehr ausgeführt.

Service Worker sind eigene Prozesse die in einem anderen Kontext laufen als die eigentliche Webseite. Einmal registriert existieren sie und fungieren als proxy, unabhängig davon ob die Webseite gerade geladen ist oder nicht. Besucht ein Nutzer die Seite wird der Service Worker geladen. Kehrt er wieder so ist der Service Worker bereits aktiv und kann Anfragen des Browsers abfangen. Da einer der Hauptanwendungsfälle für Service Worker das Offline verfügbar machen von Webanwendungen ist, verfügen sie über Unterstützung von Caching-APIs. Durch die Caching-API ist es möglich Anfragen zu speichern und zu einem späteren Zeitpunkt wieder abzurufen. Somit ist es nicht nur möglich eigene Anfragen aus dem Cache zu beantworten, sondern ebenfalls gespeicherte Ressourcen an andere Clients auf Anfrage weiter zu leiten. Daher eigenen sie sich gut für die Verwendung als Proxy in einem Client-seitiegen CDN.

- request reihenfolge
- https://vanseodesign.com/web-design/browser-requests/
- html dokument
- script tags
- bilder
- js wird geladen
- wie als requests die als script tag eingebunden werden abfangen?
- abfangen mit jsavascript event im page context nicht möglich
- kein handler
- durch timing unmöglich
- turbolinks verhindert page load und mach anfragen per ajax
- - mit eigenen tags späteres manuelles laden von ressourcen möglich
- - hoher anpassungsbedarf auf anwendungsseite...
- websockets
- eigener Prozess
- sind zur ladezeit der seite bereits verfügbar

4.4 VERBINDEN VON PEERS

- Signaling
- faye
- über Websocket channel
- Websockets werden verwendet um Verbindungen aufzubauen
- Danach Webrtc zum direkten herstellen der Verbindung
- Anwendungslogick
-

4.5 MESH ZUORDNUNG

Im Folgenden werden verschiedene Zuordnungsstragien zur Bildung von Peer Meshes diskutiert. Dazu wird der typische Workload beider Anwendungen analysiert um eine jeweils geeignete Strategie zu wählen.
- Vergleich von Meshing verfahren/peer routing aus literatur

4.5.1 *Routing*

Im Folgenden werden verschiedene Routing Peer To Peer Routing Algorithmen aus der Literatur vorgestellt und diskutiert welcher Ansatz für die betrachteten Anwendungsfälle am geeignetsten ist.

- Datenstruktur
- Dezentralisierte Datenspeicherung
- Daten werden über SPeicherknoten verteilt
- Jeder Knoten eintrag in Hashtabelle
- direct storage: Daten in Hashtabelle
- nur für kleine Daten
- indirect storage: Verweis auf daten in Hashtabelle
- Eigenschaften: Fehlertoleranz Lastenverteilung Robustheit Selbstorganisation Skalierbarkeit
- consistent hashing
- Server zum routen https://www.coralcdn.org/pubs/

4.5.1.1 *Chord*

How to save files in advance??? save file references

4.5.1.2 *Kademlia*

4.5.1.3 *IPFS*

4.5.1.4 *Kelips*

4.5.1.5 *Pastry*

4.5.2 *Schul-Cloud*

Analyse workload mit grafik

- Schulcloud
-

Schulcloud - Global einfache umsetzung Kurs unabhänige assets können geteilt werden Maximale Mesh größe Mehrere Meshes nötig Möglicherweise nicht im Mesh mit relevanten Peers Maximiert die Anzahl der Peers pro Mesh Wahrscheinlichkeit für selbes Subnetz eher gering Funktioniert auch mit wenigen Clients Ineffektiv wenn viele Clients vorhanden sind

- Schule Einfache Umsetzung Funktioniert auch mit wenigen Clients Relativ hohe trefferrate da schulen selten mehr als 1000 Schüler hat Max mesh größe um die 256(Chrome) Relativ wahrscheinlich gleiches Subnetz

- Kurs Hohe trefferrate Kleine Meshes benötigt mehr Clients Relativ wahrscheinlich gleiches Subnetz –> Daten die das bestätigen

hybride Ansätze: Zwei priorisierte Meshes Schule und Klasse

Berechnung eines Scores für jeden Peer: Möglichst viele gemeinsame kurse Liste von Kursen für jeden Peer Schnittmenge für jeden peer der online ist bilden Kardinalität der Menge = Score von Peer Rechenaufwendig Aber machbar Beste Trefferrate Funktioniert wenn wenige und wenn viele Peers anwesend sind

4.5.3 *Slidesync*

Slidesync ist eine Plattform deren Nutzung stark durch die durchgeführten live Events dominiert wird. Ein Moderator erstellt das Event lädt die notwendigen Assets, z.B. Foliensätze, hoch. Live Events werden für eine bestimmte Zeit festgesetzt und Teilnehmer laden zum start des Events die Seite. Ein Großteil des entstandenen Traffics besteht aus HLS Videoseqmenten. Jeder Teilnehmer eines Events benötigt die selben Inhalte. *Grafik visits* *Grafik traffic*

Die Peer Meshes in Slidesync werden als voll vermaschte Netzte abgebildet. Da alle Teilnehmer eines Events zu großen Teilen die selben Daten benötigen können sie in dem selben Mesh untergebracht werden. Um zu gewährleisten das sich die Peers im Selben Subnetz befinden teilen sich nur solche ein Peer Mesh die sich in der Selben IP Range befinden. Ein weiterer wichtiger Factor ist der Kommunkationsoverhead der durch das halten von Verbindungen zu vielen Peers entsteht. Deshalb ist es nicht möglich bei größeren Events alle Peers im selben Peer Mesh unter zu bringen. Deshalb werden Sub Meshes gebildet in denen sich eine maximale Anzahl an Peers befinden können.

Abbildung 7 zeigt eine beispielhafte Aufteilung von Peer Meshes für ein Event. Für Netzwerk A und B werden jeweils zwei Meshes erzeugt und nur solche Clients werden miteinander verbunden die sich auch im Selben Subnetz befinden. Jedes Netzwerk wird wiederum in zwei Sub-Meshes unterteilt.

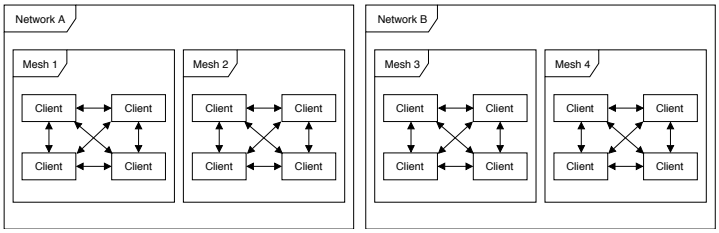

Figure 7: Peer to Peer Meshes - Slidesync

- Aussortieren von alten peers
- Background Job
- Job wird gestartet wenn kein freies Mesh verfügbar ist
- Peers senden regelmäßig ping an server
- Kommt ping nicht mehr wird angenommen Peer das Peer offline ist
- Unterstützt ein Peer Browser das CDN nicht wird kein Ping mehr gesendet

4.6 ROUTING - FINDEN VON RESSOURCEN

Um das Peer To Peer Netzwerk als CDN Nutzbar zu machen ist es wichtig das ein Peer in der Lage ist herauszufinden wer welche resource bereitstellt. Dazu lassen sich verschiedene Ansätze verfolgen.

DHT

distributed hash tables erklären

Structured vs untructured

Da das Routing von Ressourcen bei den Betrachteten Anwendungsfällen in einem Zeitkritischen Moment erfolgen muss wurde sich

für einen anderen Ansatz entschieden. Jeder Peer hält eine Hashtabelle mit den Ressourcen seiner Peers vor. Fügt ein Peer eine neue Ressource zu seinem Cache hinzu oder entfernt sie muss er alle verbundenen Peers über diese Änderung informieren. Dadurch muss im Falle einer Anfrage nicht erst die Ressource im Netzwerk gesucht werden. Dies ist möglich durch die Struktur des Netzwerkes. Da nicht alle Peers miteinander verbunden sind sondern voll vermaschte submeshes gebildet werden ist es möglich alle relevanten Peers über Änderungen zu informieren. Dadurch ist es möglich die Rechenleistung für das auffinden von Ressourcen in einen weniger Zeitkritischen Moment zu verlagern. Jedoch hat dies zur Folge das die Meshes so gebildet werden müssen das die Peers möglichst viele Ressourcen gemeinsam benötigen. Ist eine Ressource nicht im Mesh vorhanden kann sie vom Server geladen werden. *Duplicate*

4.6.1 *Updates*

- Diagramm
- Client lädt ressource
- Client cached Resource
- Sendet nachricht an peers das Resource gecached wurde und verfügbar ist
- Clients speicher Client Resource hash in Hashmap

4.6.2 *Subnetzerkennung*

- Routing ohne NAT Server
- Subnetze von Organisationen bekannt
- Peer Mehses bilden in denen nur Peer aus dem Subnetz sind

4.7 WIEDERVERWENDBARKEIT

4.8 OPEN SOURCE

- evtl. Open source erklären
- bereitstellung für die öffentlichkeit
- Welche Lizenz?

4.9 OFFLINE SUPPORT

- Motivation: Internet in Schulen ist nicht immer verfügbar

- wie funktionieren offline webanwendungen
- Live Streams: Ausfallsicherheit wird erhöht.
- quasi bei design
- Resourcen werden gecached und sind offline verfügbar
- Tobias arbeit Refernzieren
- Übertragung im lokalen Netzwerk möglich wenn verbindung aufgebaut ist
- Signaling müsste in lokalem netzwerk sein z.b. Rechner vom Lehrer
- evt. browser plugin
- Wie das routing machen?
- Offline scenario:
- Lehrer Lädt ressourcen vor und macht sie für schüler verfügbar
- Kein Internet vorhanden
- Schüler laden Ressourcen von Lehrer

4.10 SECURITY

- Owasp
- https://www.owasp.org/images/9/90/OWASP$_{T}$op$_{1}$0−2017$_{d}$e$_{V}$1.0.pdfIPLeakmöglich

- Stun Server kann nach IP Adresse fragen
- Über js auslesbar
- Pluckins können das blocken
- media.peerconnection.enabled ausschalten
- –> kein webrtc mehr möglich
-
- Datenintegrität integrity
- Integrität des kommunikationspartners confidentiality
- –vertrauensumgebung??
- availability
- durch hybrid cdn

- fallback lösung
- authenticity
- kann durch authority gelöst werden
- non repudiation
- accountability
- kann mit Statistiken getrackt werden
-
- Datachannel ist verschlüsselt
- https notwendig
- websocket ist verschlüsselt

5

IMPLEMENTIERUNG

5.1 ARCHITECTUR

- Technologiewahl
- ES6 compilation
- Beschreibung der Komponenten:
- Service Worker
- Cached Ressourcen
- Proxy
- P2PCDN
- Schnittstelle für externe Anwendungen
- Nimmt Konfiguration entgegen
- Initialisiert CDN
- Middleware
- Vermittler zwischen Service Worker und Script
- Arbeitet mit Events
- Welche Events gibt es wer registriert sich drauf?
- Peer
- Representiert eigenen Peer
- Hält verbindungen zu anderen Peers
- Signaling
- FayeConnection

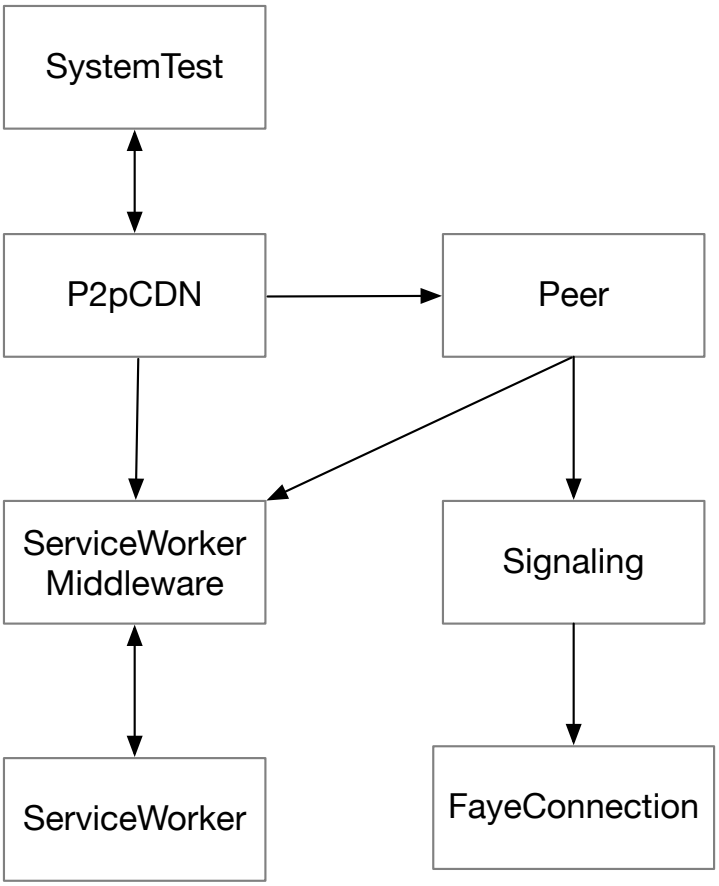

Figure 8: Klassendiagramm

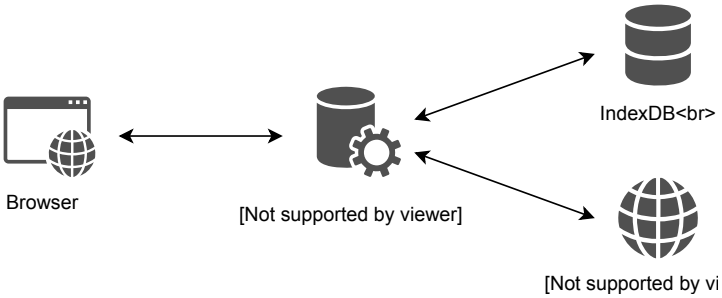

Figure 9: A Figure Title

5.1.1 *Service worker*

- warten bis sw active ist/alle verbindungen ready sind vs request normal durchgehen lassen bis alles fertig ist.
- Austausch erst möglich wenn script geladen ist
- blockent:
- Ressourcen werden so lange aufgehalten bis verbindung initialisiert

- –> längere Ladezeiten
- mehr Bandbreite kann gespart werden
- nicht blockent:
- Ressourcen werden über server geladen bis verbinungen aufgebaut sind
- Weniger Bandbreite wird gespart
- Ladezeit wird nicht verzögert
- Heartbeat um zu überprüfen ob script geladen ist
- Mehrere Tabs?
-
- first page load
- Single page apps
- Turbolinks
- Requests werden erst nach erfolgreicher registrierung behandelt
- clients.claim + skip waiting für den ersten aufruf (12)
- Codebeispiel für wartende messages
- Callbacks

5.1.2 *Tests*

Um das Plugin zu testen wird als test runner karma verwendet.[1] Als test framework wird mocha[2] und als assertion Library wird Chai[3] eingesetzt

5.2 RESSOURCEN MANAGEMENT

5.3 CONFIGURATION

Um eine gute Anpassung an verschiedene Anwendungsfälle zu ermöglichen bietet das Peer To Peer CDN eine Reihe von Konfigurationsmöglichkeiten. Nachdem das Client Script die Konfiguration geladen hat wird sie im der Indexed DB gespeichert und von dort durch den Service Worker geladen.1 zeigt eine Beispielhaft Konfiguration des CDNs im Folgenden werden die verschiedenen Konfigurationsmöglichkeiten aufgelistet und beschrieben.

1 https://karma-runner.github.io/latest/index.html
2 https://mochajs.org/
3 https://www.chaijs.com/

```
var config = {
  channel: 'FIXED_CLASS_1',
  clientId: '<%= peerId %>',
  idLength: 32,
  stunServer: {
    'iceServers': [
      // {
      //   'urls': 'stun:stun.l.google.com:19302',
      // },
    ]
  },
  verbose: true,
  serviceWorker: {
    urlsToShare:
      [
        '/img/',
        '/video/',
        '/testfiles/'
      ],
    path: '/p2pCDNsw.js',
    scope: '/',
    basePath: '/',
    storageQuota: '10000',
    cachingEnabled: false,
    verbose: true,
    statisticPath: '/logs'
  }
};
var cdn = new P2pCDN(config);
```

Listing 1: Beispielhafte Konfiguration

CHANNEL
: Bezeichnet den für das Peer Meshing zu verwendenden Websocket channel. Alle Clients mit dem selben Channel befinden sich im selben Peer Mesh.

CLIENTID
: Eindeutiger Identifier mit dem der Peer identifiziert werden kann. Ähnlich einer Session ID wird er verwendet um Clients wieder zuerkennen und anzusprechen.

IDLENGTH
: Bezeichnet die maximale Länge der ClientIds. Kürzere ClientIds werden bis zu dieser Länge aufgefüllt. Wird benötigt um

intern bei dem verschicken von Packeten über das CDN ClientIds fester länge verwenden zu können.(siehe) *referenzieren*

STUNSERVER
: Gibt den zu verwendenden STUN Server an. Dies kann ein öffentlicher oder privat betriebener Server sein. Kann freigelassen werden falls kein STUN Server verwendet werden soll

VERBOSE
: Aktiviert/deaktiviert Debug Ausgaben.

SERVICEWORKER
: Beinhaltet alle Konfigurationen die den Service Worker betreffen.

URLSTOSHARE
: Liste aller URL die mit Hilfe des CDN bearbeitet werden sollen.

EXCLUDEDURLS
: Liste von URLs die explizit von dem CDN ausgeschlossen werden sollen

PATH
: und Text dahinter Pfad von dem das Service Worker Script geladen werden soll.

SCOPE
: Gibt den Scope an unter dem der Service Worker arbeiten soll.

BASEPATH
: Gibt den Service Worker Base Path an.

STORAGEQUOTA
: Maximal für das CDN zu verwendender Cache Speicher. Überschreitet der Cache den Wert, werden so lange Ressourcen aus dem Cache gelöscht bis der Wert unterschritten ist. (siehe) *ref*

CACHINGENABLED
: Aktiviert/Deaktiviert das Caching innerhalb des Service Workers. Nützlich zum Debuggen.

VERBOSE
: Gibt an ob der Service Worker debugging Ausgaben auf die Konsole schreiben soll.

STATISTICPATH
: URL an die die erhobenen Statistiken gesendet werden sollen. siehe 5.11

5.4 CLIENT UI EVENT

Um es der einbindenden Anwendung zu ermöglichen auf Änderungen bezüglich der verbundenen Peers sowie deren Ressourcen zu Reagieren stellt das Plugin das Event ui:onUpdate bereit das bei Änderungen ausgelöst wird. Das Event übergibt das Peer Object des Clients wodurch der Event empfänger zugriff auf die Anzahl der verbundenen Peers so wie deren Ressourcen hat.

5.5 SIGNALING SERVER

The signaling server itself uses socket.io and can be found here. The client ID is created there and is essential for the lifecycle of a peer in the whole network. It is not clear if the client IDs given by socket.io always have the same length. Therefore, client IDs will be padded to a maximal length of 24. This is necessary because the client IDs need to be sent via the binary datachannel and consequently, this requires a fixed length.

- websockets faye
- gleicher data channel zur Bildung von meshs
- ID pro client
- max id length muss festgelegt werden für chunking
- Protokoll von P2PCDN umgesetzt
- Protokoll erklären
- Diagram Protokoll
- Peer Meshing wird von anwendung übernommen

5.5.1 *Slidesync*

- Rails Model
- Code Beispiel
- Tracking in Redis welcher Peer in welchem Submesh ist
- Peer wird aus liste nicht voller mehses gewählt
- Falls alle voll sind wird neues Mesh angelegt und garbage collection gestartet.
- Datentyen und mapping erklären
- Background job räumt leere meshes auf (Garbage collection)
- löscht leere meshes aus liste

5.5.2 *Schul-Cloud*

5.6 MESSAGE PROTOCOL

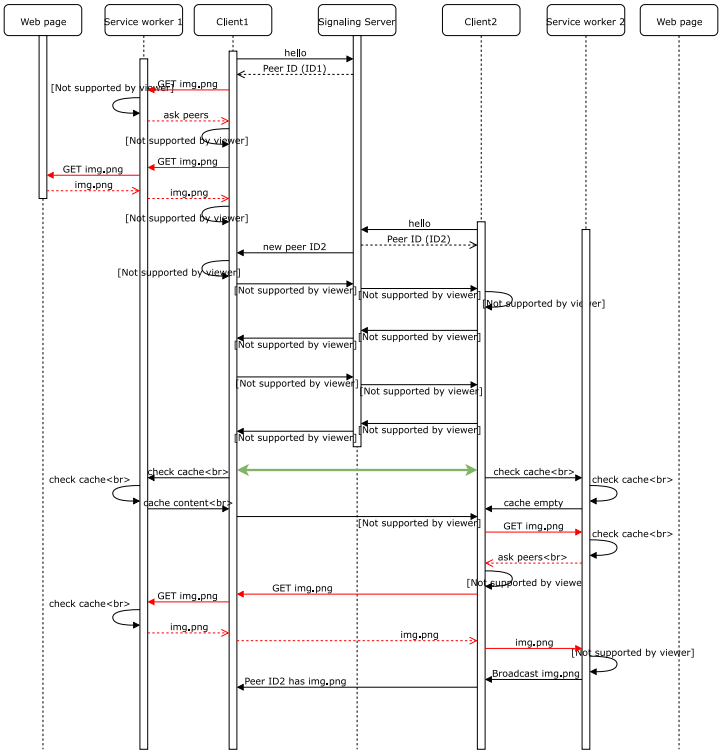

Figure 10: A Figure Title

Diagramm aktualisieren

5.6.1 *Updates*

- message types
- neue Resource
- gelöschte Resource
- Client tritt dem Netzwerk bei
- Client verlässt Netzwerk
- Diagram aktualisieren
- alle Clients müssen benachrichtigt werden
- Über Webrtc data channel
- Message format zeigen

5.6.2 *Client fragt Ressource an*

- Message Format
- Diagram beschreiben

5.7 MESH ZUORDNUNG

5.8 REUSABILITY

5.9 SERIALISIERUNG DER DATEN

Für den Austausch von Daten werden die von WebRTC angebotene DataChannel genutzt, welche das Stream Control Transmission Protocol kurz SCTP verwendet. Problem hierbei ist, dass dieses Protokoll ursprünglich für die Übertragung von Kontrollinformationen designt wurde und deshalb für die Kompatibilität verschiedener Browser eine Paketgröße von 16kiB nicht überschritten werden sollte. Es ist jedoch notwendig auch größere Dateien zu übertragen, weshalb aktuell viele kleine Datenpakete verwendet werden müssen. Hierdurch entsteht ein nicht zu vernachlässigender Overhead.

```
1  // maximum buffer size is 16mb
2  if(peer.dataChannel.bufferedAmount <= 16000000) {
3    peer.dataChannel.send(msg);
4    return;
5  }
6  // if maximum buffersize is reached delay sending of chunks
7  peer.requestQueue.push(msg);
8  peer.dataChannel.bufferedAmountLowThreshold = 65536;
9  peer.dataChannel.onbufferedamountlow = function () {
10   var reqs = peer.requestQueue.slice();
11   peer.requestQueue = [];
12   reqs.forEach(_msg => send(_msg));
13 }
```

Listing 2: Buffersize berücksichtigung

- SCTP(DataChannel) message size limit 16kiB
- Fixe id länge notwendig
- datachannel buffersize muss berücksichtigt werden
- chunking reassembling nötig
- Performance einbussen

```
_handleChunk(message) {
  const req = this._getRequest(message.from, message.hash);
  var response = {}
  req.chunks.push({id: message.chunkId, data:
  ↪  message.data});

  if(req.chunks.length === message.chunkCount) {
    response.data = this._concatMessage(req.chunks)
    response.from = message.from;
    response.peerId = this.peerId;
    this._removeRequest(message.from, message.hash);
    req.respond(response);
  }
}
```

Listing 3: Buffersize berücksichtigung

- abToMessage und sendToPeer
- Details zum Algorithmus

5.10 SYSTEM TEST

Das Plugin stellt ein Modul bereit um zu testen ob es einem Client möglich ist am Peer To Peer CDN teilzunehmen.

Dazu werden drei tests bereitgestellt.

p2pCDN.systemTest.testBrowser()

Mit Hilfe von modernizr[4] testet die Funktion ob die verwendete Browserversion alle benötigeten Funktionen unterstützt. Modernizr ist eine Javascript Bibliothek mit der gestetet werden kann ob ein Browser bestimmte funktionen unterstützt.

p2pCDN.systemTest.webrtcInitialized()

Gibt ein Promise zurück welches überprüft ob die webrtc Verbindung erfolgreich aufgebaut wurde. Da die Initialisierung einen moment in Anspruch nehmen kann wird wiederholt geprüft ob die Verbindung aufgebaut wurde.

p2pCDN.systemTest.clientConnected()

Gibt ebenfalls ein Promise zurück und überprüft ob erfolgreich eine Verbindung zu einem anderen Client aufgebaut werden konnte. Um diesen Test erfolgreich auszuführen muss sich ein andere Client im aktuellen Peer mesh befinden.

4 https://modernizr.com/

5.11 ERFASSEN VON STATISTIKEN

```
function sendStatisticToServer() {
  if(!serverSendTimeout && config.statisticPath){
    serverSendTimeout = setTimeout(function(){
      try {
        fetch(config.statisticPath, {
          method: 'POST',
          body: JSON.stringify(requests),
          headers:{
            'Content-Type': 'application/json'
          }
        });
      } catch(e) {

      } finally {
        serverSendTimeout = 0;
        requests = [];
      }
    }, sendStatisticDelay)
  }
}
```

Listing 4: Erfassen der Statistiken

Um die Nutzungsstatistiken des CDNs zu erfassen sendet jeder client periodisch POST requests an den Server. Dazu sammelt der Service Worker alle Anfragen die in einem Zeitraum von 10 Sekunden angefallen sind und sendet sie gebündelt als JSON an den Server. Erfasst werden:

PEERID
: Die PeerId bezeichnet die Id des peers der die Statistik sendet.

METHOD
: Method gibt an wie die Anfrage behandelt wurde und kann die Werte 'cacheResponse', 'peerResponse' oder 'serverResponse' beinhalten. Ein cacheResponse konnte aus dem eigenen Cache beantwortet werden. ServerResponse bedeutet das die Anfrage über den externen Server geladen werden musste. Der Wert peerResponse gibt an das die Anfrage über das Peer To Peer CDN bearbeitet werden konnte.

FROM
: 'From' gibt an woher die Anfrage geladen wurde. Im Falle eines serverResponses beinhaltet sie den Wert 'server' und bei einem

```
function logStatistic(url, method, request, timing, from,
↪  peerId) {
  if(!config.statisticPath) return;
  var p_Id = peerId ? peerId : config.clientId;
  var data = {
    'peerId': p_Id,
    'method': method,
    'from': from,
    'url': url,
    'loadTime': timing
  };
  requests.push(data);
  sendStatisticToServer();
}
```

Listing 5: Erfassen der Statistiken

cacheResponse den Wert cache. Wurde die Anfrage über das Peer To Peer Netzwerk beantwortet beinhaltet sie die peerId des Peers der die Anfrage beantwortet hat. Dazu sendet das Script neben der eigentlichen Anfrage auch die eigene PeerId und die PeerId des peers der die Anfrage beantwortet hat an die Service Worker. (siehe 7)

URL
: Die URL enthält die URL der angefragten Ressource.

TIMING
: Timing beinhaltet die Zeitspanne die benötigt wurde um die Anfrage zu beantworten, beginnend vor der Entscheidung wie der Request abgearbeitet werden soll(siehe 6) und endend nach dem die Anfrage empfangen wurde. Nicht enthalten in der Zeitspanne ist die Entscheidung ob der Service worker den Request bearbeitet und die Renderzeiten des Browsers. Diese Zeiten sind nicht abhänig von der Art der Request Beantwortung.(siehe evaluation)

Mit Hilfe der Configuration kann festgelegt werden an welchen Endpunkt die Statistik gesendet werden soll. Die Anwendung ist für das speichern und verarbeiten der Daten zuständig, dies ist nicht Teil des Plugins. Slidesync speichert die Daten als JSON in Redis und stellt einen JSON Endpunkt zur Verfügung mit dem die Statistiken abgerufen werden können. Für die Labortests werden die Daten in JSON Dateien zur späteren Verarbeitung abgelegt.

- evtl. Mongo db

- anzeigetool
- schoolcloud

5.12 QUOTA LIMITS - LÖSCHEN VON REQUESTS AUS DEM CACHE

Table 2: Browser Storage Quotas [5]

Browser	Limit
Chrome	< 6% des freien Fesplattenspeichers
Firefox	< 10% des freien Fesplattenspeichers
Safari	< 50MB
IE10	< 250MB
Edge	Abhännig von der Festplattengröße

Browser stellen den Clients unterschiedlich viel Speicherplatz für offline Caches zur Verfügung. Ist das Quota limit erreicht versuchen Firefox und Chrome Speicher frei zu machen indem Elemente aus dem Cache gelöscht werden. Dabei werden jedoch keine einzelnen Elemente aus dem Cache gelöscht sondern mittels Last-recently-used(LRU) werden ganze Caches gelöscht. Safari und Edge haben keinen Mechanismus zum automatischen Löschen von Elementen sondern werfen lediglich einen Fehler.[6] Deshalb ist es notwendig das der Service Worker in dem Fall das das Limit erreicht wird Elemente löscht.

Mit Hilfe der Quota Management API[7] ist es möglich die momentane Speichernutzung auszulesen ebenso wie den maximal Verfügbaren Speicherplatz. Ist diese Limit oder das Quota Limit welches über die Konfiguration angegeben wurde erreicht, löscht der Service Worker so lange die ältesten Einträge im Cache, bis genügend Speicher für den nächsten Request vorhanden ist. Dazu berechnet der Service Worker die Größe des zu speichernden Request.

5.13 RESOURCE LOADING

6 https://developers.google.com/web/fundamentals/instant-and-offline/web-storage/offline-for-pwa

7 https://developers.google.com/web/updates/2011/11/Quota-Management-API-Fast-Facts

```
function handleRequest(url, clientId) {
  return new Promise((resolve) => {
    var startTime = performance.now();

    sha256(url).then(hash => {

      // check cache
      getFromCache(hash).then(cacheResponse => {
        if (cacheResponse && config.cachingEnabled) {
          log('cacheResponse ' + cacheResponse.url);

          // This notify should not be needed
          notifyPeersAboutAdd(hash, clientId);
          var endTime = performance.now();
          logStatistic(url, 'cacheResponse', cacheResponse,
          ↪  endTime-startTime, 'cache');
          resolve(cacheResponse);
          return;
        }
        // check peers
        getFromClient(clientId, hash).then(data => {
          if (data && data.response) {
            var peerResponse = data.response;
            log('peerResponse ' + peerResponse.url);
            putIntoCache(hash, peerResponse, clientId);
            notifyPeersAboutAdd(hash, clientId);
            var endTime = performance.now();
            logStatistic(
              url,
              'peerResponse',
              peerResponse,
              endTime-startTime,
              data.from,
              data.peerId
            );
            resolve(peerResponse);
            return;
          }
          // get from the internet
          getFromInternet(url).then(response => {
            log('serverResponse ' + response.url);
            putIntoCache(hash, response, clientId);
            notifyPeersAboutAdd(hash, clientId);
            var endTime = performance.now();
            logStatistic(url, 'serverResponse', response,
            ↪  endTime-startTime, 'server');
            resolve(response);
          });
        });
      });
    });
  });
}
```

```
_handleChunk(message) {
  const req = this._getRequest(message.from, message.hash);
  var response = {}
  req.chunks.push({id: message.chunkId, data:
  ↪  message.data});

  if(req.chunks.length === message.chunkCount) {
    response.data = this._concatMessage(req.chunks)
    response.from = message.from;
    response.peerId = this.peerId;
    this._removeRequest(message.from, message.hash);
    req.respond(response);
  }
}
```

Listing 7

6

EVALUATION

6.1 PREQUISITES

6.2 BROWSER COMPATBILITY

- Kein IE
- Edge nur in neuer version mit chrome dahinter
- Chrome
- Firefox
- Analyse von verwendeten Clients aktueller Events

6.2.1 *Browser Usage in coropate networks*

- Statistic über typische nutzung
- Statistic über Nutzung bei dem test
- Diskussion Edge on Chromium
- evtl aussage von deutscher bank mit aufnehmen
- — major update hinauszögern, in 1-2 Jahren
-

6.2.1.1 *Chunking*

- messen des aufwandes für chunking und wieder zusammensetzen
- woher kommt der zusätzliche Aufwand bei größen dateien??

6.2.2 *Browser usage in eduational networks*

6.3 BANDWIDTH

6.3.1 *Simulierter Workload*

- batches
- gleicher Zeitabstand gleiche Client zahl
- Random client ankunft
- Future Soc lab

6.3.1.1 *Datei größen*

- Mac book pro Ende 2013
- 2.3 ghz i7
- 16gb ram
- 1, 5, 10, 20, 30, 40, 50, 60, 70, 80, 90 , 100 mb
- durchsatz berechnen
- Limitierung durch websockets
- lokal auf einem Rechner um Netzlaufzeiten auszuklammern
- 1 Peer lädt vor
- der andere lädt von peer

6.3.2 *Educational context*

- machbarkeitstests in schule
- setup erklären

6.3.3 *Live streaming in the coporate context*

- setup erklären
- stream simuliert mit dateien simuliert
- technische probleme?

6.3.4 *Nutzerzufriedenheit*

wie soll das aussehen?

6.4 SECURITY CONSIDERATIONS

6.5 DRM LICENCING

7

CONCLUSION

- Browser nutzung

A

AN APPENDIX

Some stuff here

LIST OF FIGURES

LIST OF TABLES

LIST OF LISTINGS

DECLARATION OF ORIGINALITY

I hereby declare that I have prepared this master's thesis myself and without inadmissible assistance. I certify that all citations and contributions by other authors used in the thesis or which led to the ideas behind the thesis have been properly identified and referenced in written form. I also warrant that the above statement applies to the implementation of the project.

Hiermit versichere ich, dass ich die Masterarbeit selbständig und ohne unzulässige Hilfe Anderer angefertigt habe und dass ich alle von anderen Autoren wörtlich übernommenen Stellen wie auch die sich an die Gedankengänge anderer Autoren eng anlehnenden Ausführungen meiner Arbeit besonders gekennzeichnet und die entsprechenden Quellen angegeben habe. Ich erkläre hiermit weiterhin die Gültigkeit dieser Aussage für die Implementierung des Projektes.

Potsdam, October 5th, 2016

Tim Friedrich