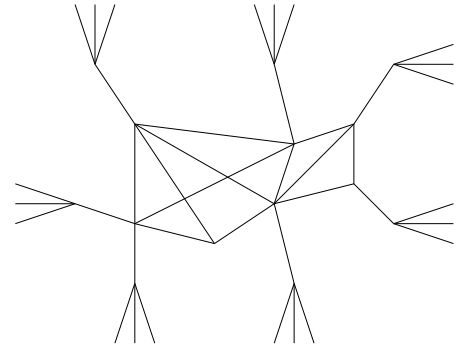
Mit wem redet mein Rechner —

Transit-Traffic durch Browser und was man damit anstellen kann

Matthias Bauer

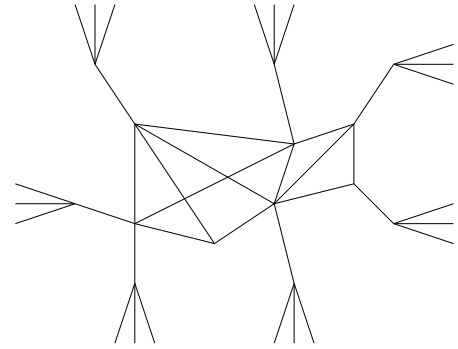
m@saeftl.franken.de

Netzstruktur



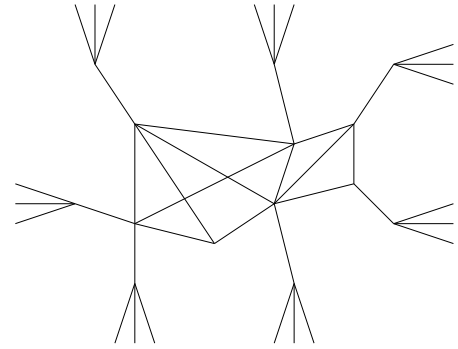
- Maschinen sind Hosts oder Router

Netzstruktur



- Maschinen sind Hosts oder Router
- Router transportieren Datagramme für Hosts

Netzstruktur



- Maschinen sind Hosts oder Router
- Router transportieren Datagramme für Hosts
- *Meine Kiste ist kein Router, also transportiert sie auch keine Daten für andere (???)*

Transit Traffic rechtlich

- Wer Daten für andere weiterleitet, haftet nach IuKDG erstmal nicht für den Inhalt

Transit Traffic rechtlich

- Wer Daten für andere weiterleitet, haftet nach IuKDG erstmal nicht für den Inhalt
- Rechtsprechung zu Würmern, etc. läuft ähnlich

Transit Traffic rechtlich

- Wer Daten für andere weiterleitet, haftet nach IuKDG erstmal nicht für den Inhalt
- Rechtsprechung zu Würmern, etc. läuft ähnlich
- Grauzone Gnutella, FreeNet, Onion Routing etc

Transit Traffic auf Hosts

- HTTP `CONNECT` bei Servern und Proxies

Transit Traffic auf Hosts

- HTTP `CONNECT` bei Servern und Proxies
- Obskure Features in FTP

Transit Traffic auf Hosts

- HTTP `CONNECT` bei Servern und Proxies
- Obskure Features in FTP
- Ping mit gefälschter Absende Adresse

Transit Traffic auf Hosts

- HTTP `CONNECT` bei Servern und Proxies
- Obskure Features in FTP
- Ping mit gefälschter Absende Adresse
- TCP SYN von gefälschten Adressen

Transit Traffic auf Hosts

- HTTP `CONNECT` bei Servern und Proxies
- Obskure Features in FTP
- Ping mit gefälschter Absende Adresse
- TCP SYN von gefälschten Adressen
- HTTP in Browsern

Kannäle in HTTP

- Redirects

Kannäle in HTTP

- Redirects
- Cookies

Kannäle in HTTP

- Redirects
- Cookies
- Diverse HTML Tags

Kannäle in HTTP

- Redirects
- Cookies
- Diverse HTML Tags
- Active Content

Transport in Javascript

```
<html>
<head>
<script language="JavaScript"><!--
function send_mesg () {
    var message = "@MESS@";
    document.subform.message.value=message;
    document.subform.submit();
}
//--></script>
</head>

<body>
<form name="subform" method="POST" action="@URL@">
<input type=hidden name="message" value="uninitialized">
</form>
<script language="JavaScript"><!--
send_mesg();
//--></script>
</body>
</html>
```

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.
- von David Chaum, 1988

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.
- von David Chaum, 1988
- *Brief im Briefumschlag im Briefumschlag . . . und jeder macht den äussersten auf und wirft den inneren Brief wieder in den Briefkasten*.

Bekannte Techniken

- Remailer
  Cypherpunks, Mixmaster, Mixminion

Bekannte Techniken

- Remailer
  Cypherpunks, Mixmaster, Mixminion
- Onion Routing
  Crowds, JAP, tor, Skype (?)

Datentransport durch Unbeteiligte

Wenn Web Server durch Clients reden können

- ist Beobachten schwerer als bei Mixmaster o.ä.

Datentransport durch Unbeteiligte

Wenn Web Server durch Clients reden können

- ist Beobachten schwerer als bei Mixmaster o.ä.
- kann man sich als Client tarnen (*Unobservability*)

Datentransport durch Unbeteiligte

Wenn Web Server durch Clients reden können

- ist Beobachten schwerer als bei Mixmaster o.ä.
- kann man sich als Client tarnen (*Unobservability*)
- sind Knoten leichter zu betreiben als z.B. Remailer

Datentransport durch Unbeteiligte

Wenn Web Server durch Clients reden können

- ist Beobachten schwerer als bei Mixmaster o.ä.
- kann man sich als Client tarnen (*Unobservability*)
- sind Knoten leichter zu betreiben als z.B. Remailer
- bleibt die Anzahl der aktiven Benutzer unklar

Datentransport durch Unbeteiligte

Wenn Web Server durch Clients reden können

- ist Beobachten schwerer als bei Mixmaster o.ä.
- kann man sich als Client tarnen (*Unobservability*)
- sind Knoten leichter zu betreiben als z.B. Remailer
- bleibt die Anzahl der aktiven Benutzer unklar

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
  - CGI Scripte auf HTTP Servern
  - Haben public/private Keys
  - Geben Bilder und/oder Javascripts zurück
  - Haben einen Sende-Ordner
  - Speicher Nachrichten für User unter Adressen

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
  - CGI Scripte auf HTTP Servern
  - Haben public/private Keys
  - Geben Bilder und/oder Javascripts zurück
  - Haben einen Sende-Ordner
  - Speicher Nachrichten für User unter Adressen

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
- Linker
  - Betreiben ganz normale Web Pages
  - allerdings mit Links zu den Knoten
  - `<iframe src="http://node/frame.html">`

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
- Linker
  - Betreiben ganz normale Web Pages
  - allerdings mit Links zu den Knoten
  - `<iframe src="http://node/frame.html">`

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
- Linker
- Benutzer des Dienstes
  - Betreiben Knoten
  - Oder benutzen Scripten zum Verschicken/Empfangen
  - Laden ihren Mails von den Knoten

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
- Linker
- Benutzer des Dienstes
  - Betreiben Knoten
  - Oder benutzen Scripten zum Verschicken/Empfangen
  - Laden ihren Mails von den Knoten

Das Muted Posthorn Protokoll

Beteiligte Parteien:

- Knoten
- Linker
- Benutzer des Dienstes
- Unwissende Web Surfer
  - Besuchen die Seiten der Linker
  - Transportieren unabsichtlich die Nachrichten

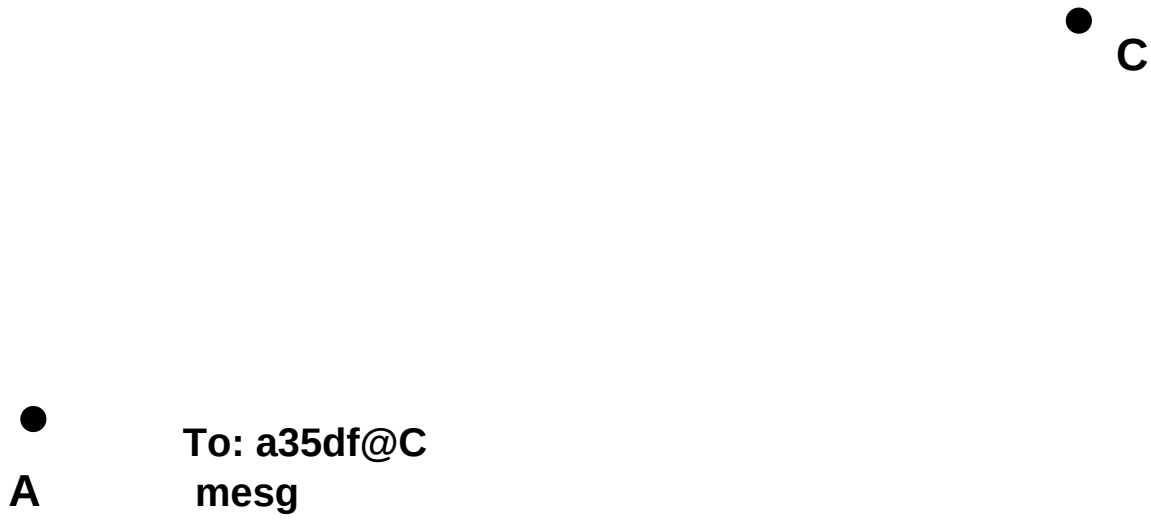
Das Muted Posthorn Protokoll

Beteiligte Parteien:

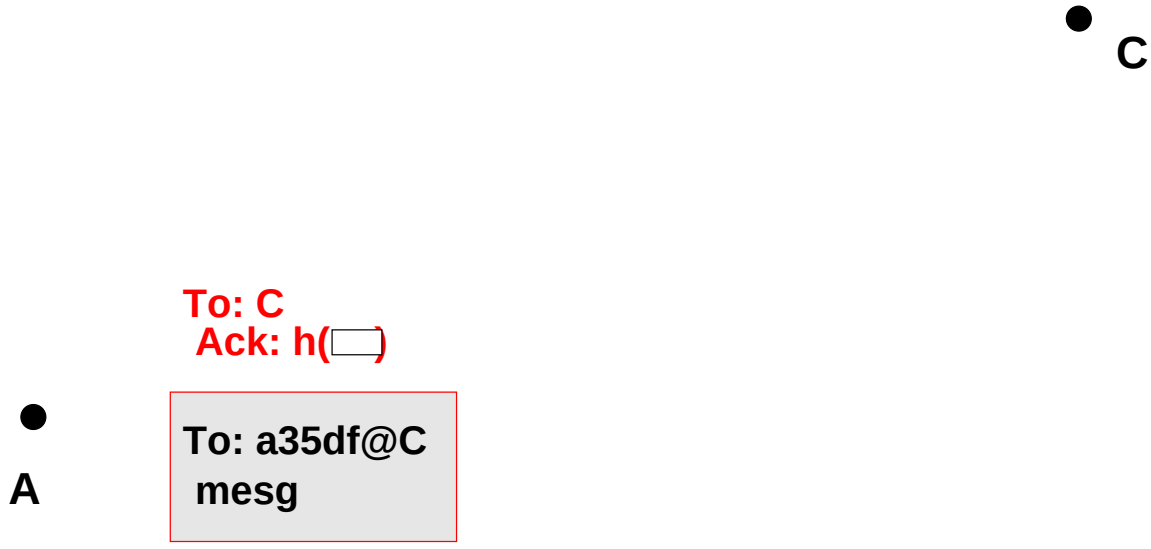
- Knoten
- Linker
- Benutzer des Dienstes
- Unwissende Web Surfer
  - Besuchen die Seiten der Linker
  - Transportieren unabsichtlich die Nachrichten

Das Protokoll in Schritten

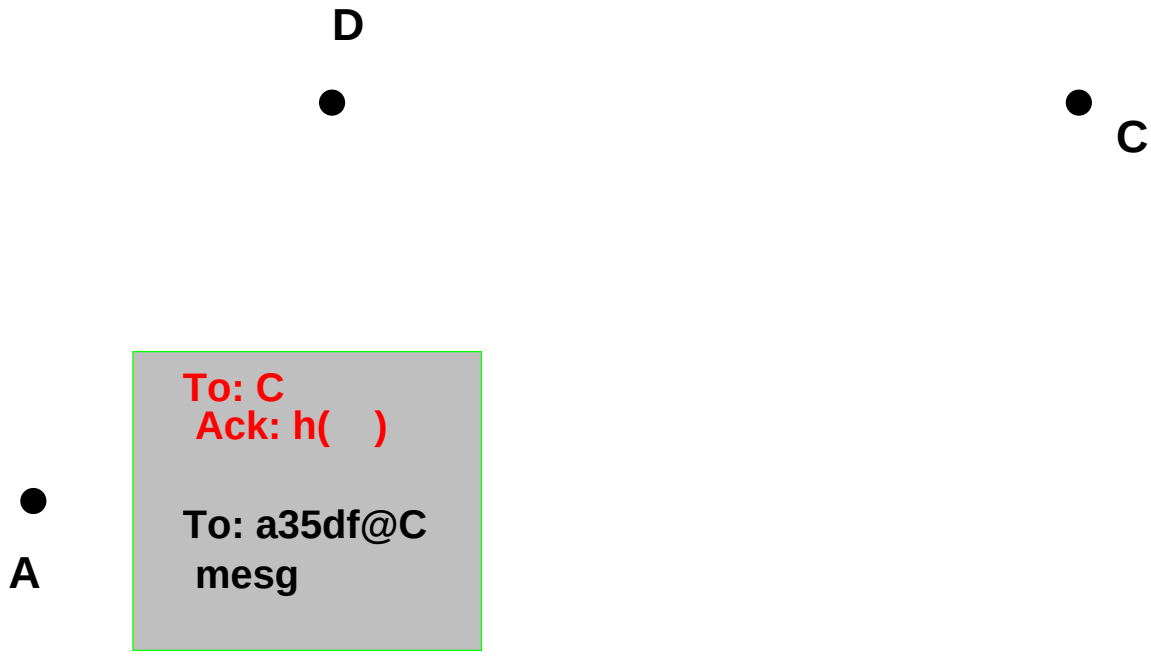
Das Protokoll in Schritten



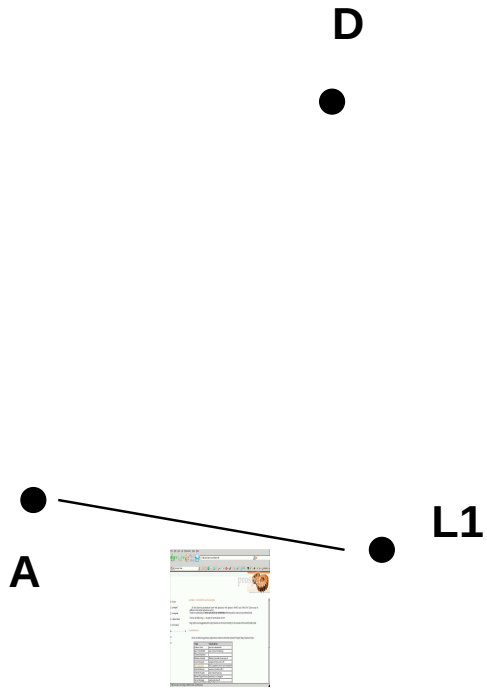
Das Protokoll in Schritten



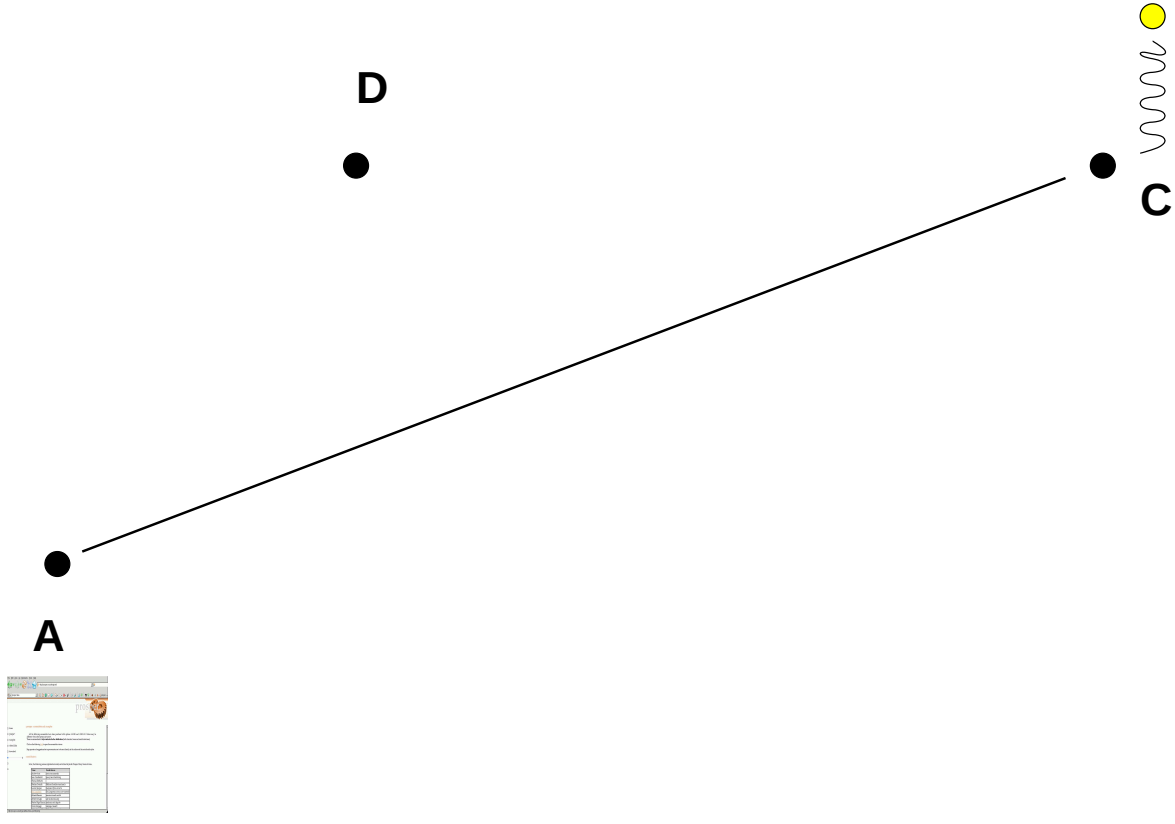
Das Protokoll in Schritten



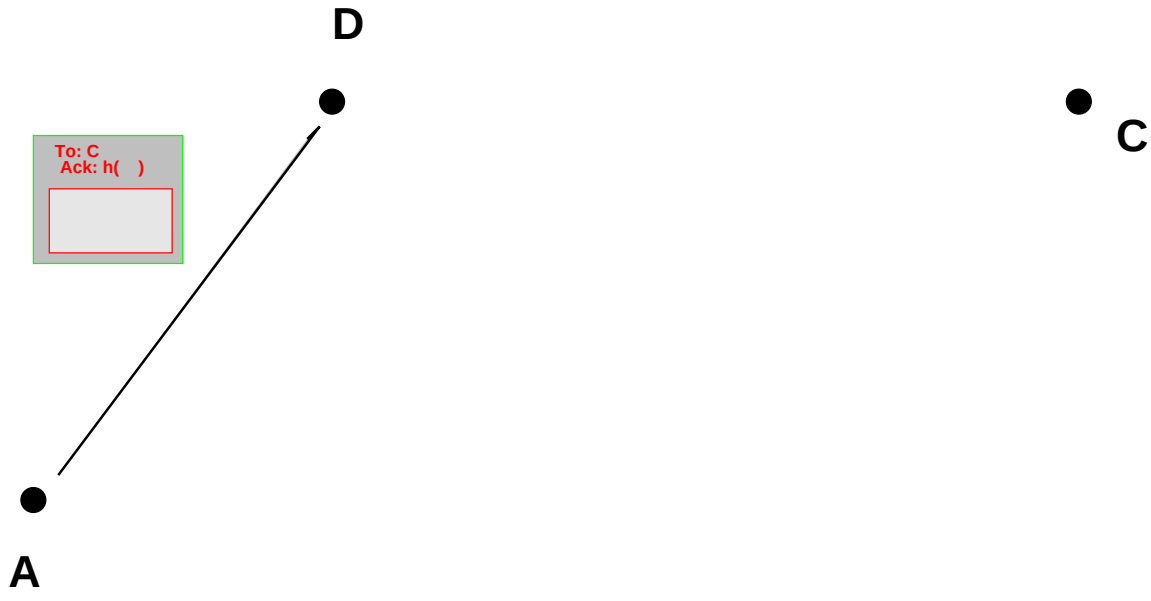
Das Protokoll in Schritten



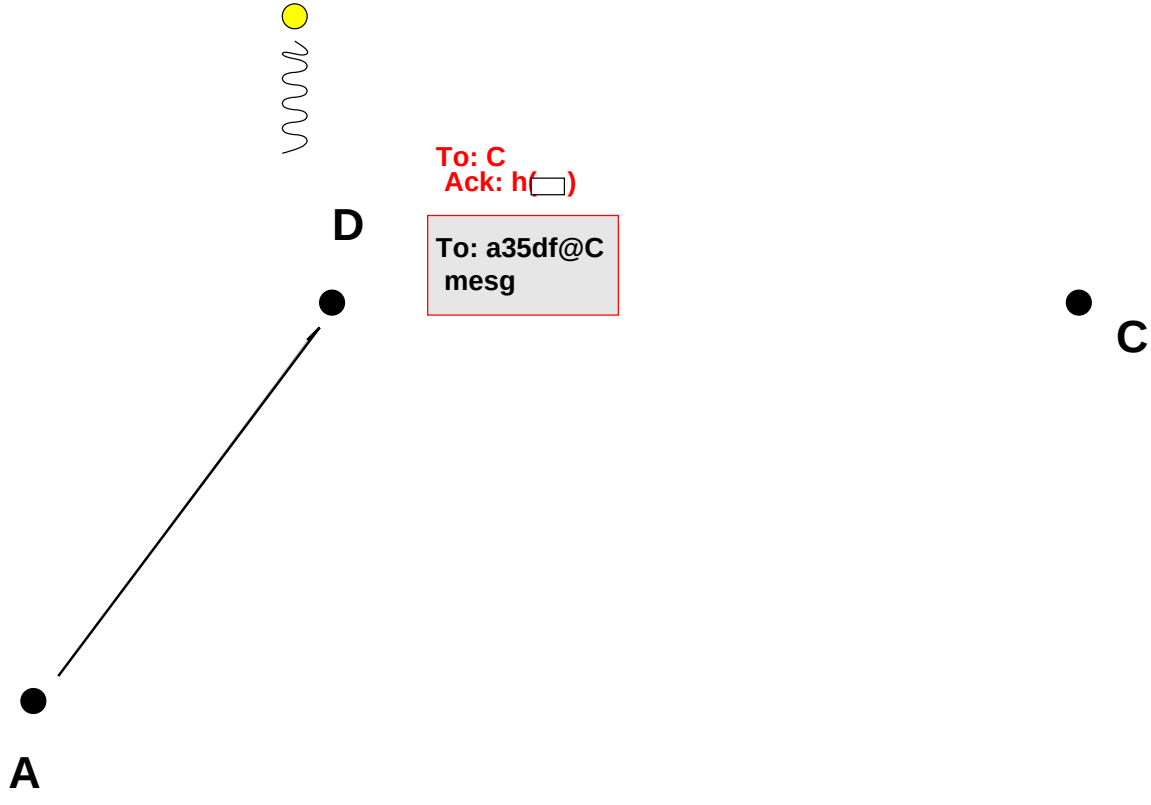
Das Protokoll in Schritten



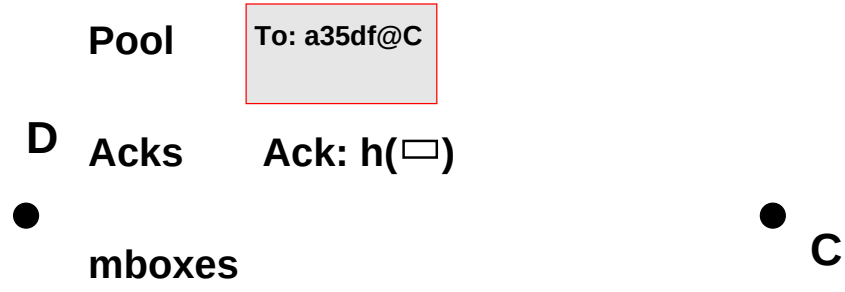
Das Protokoll in Schritten



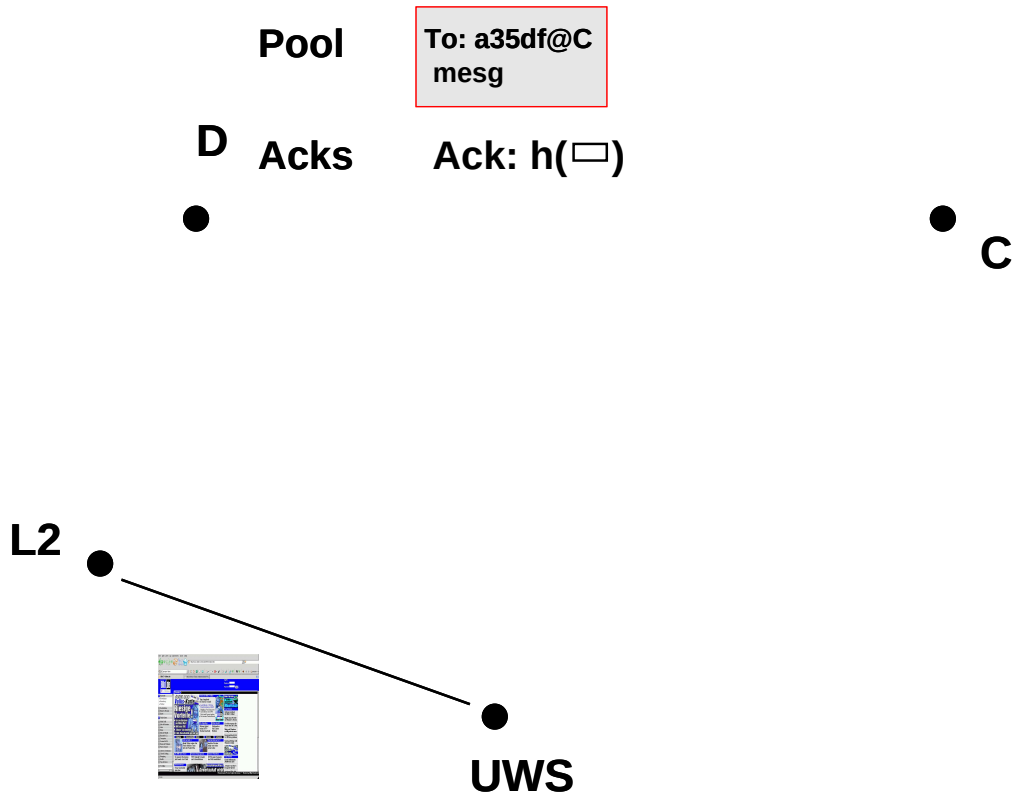
Das Protokoll in Schritten



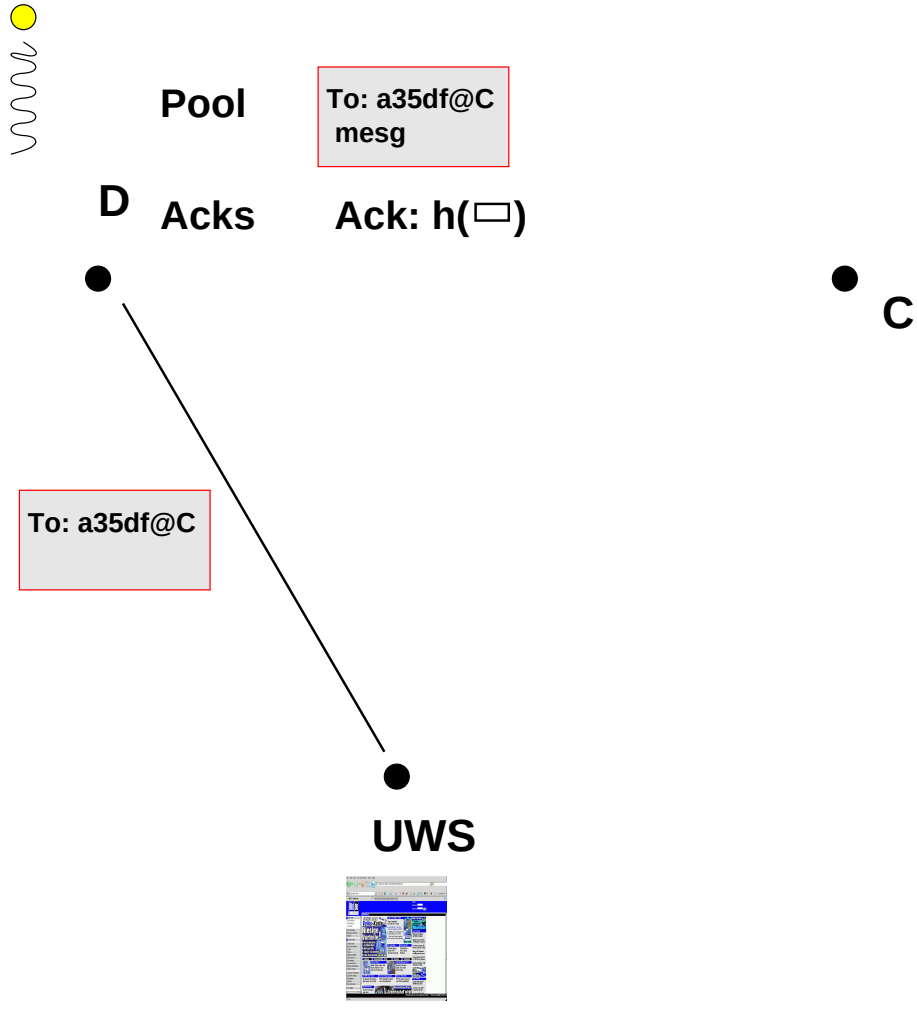
Das Protokoll in Schritten



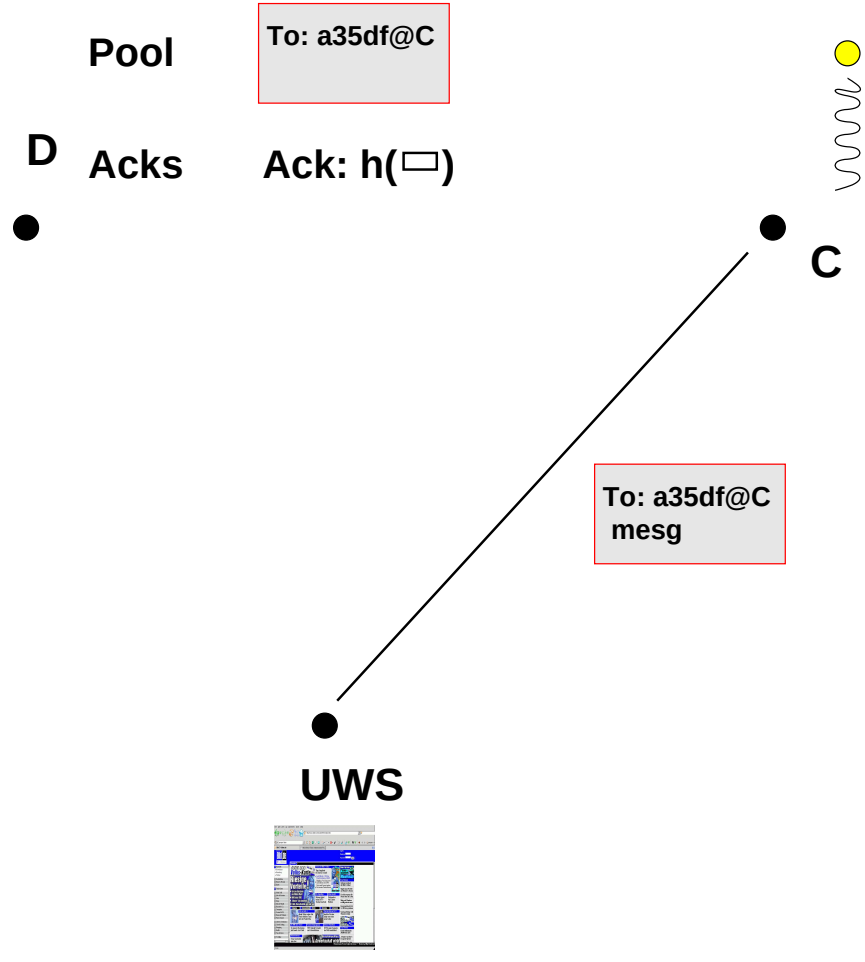
Das Protokoll in Schritten



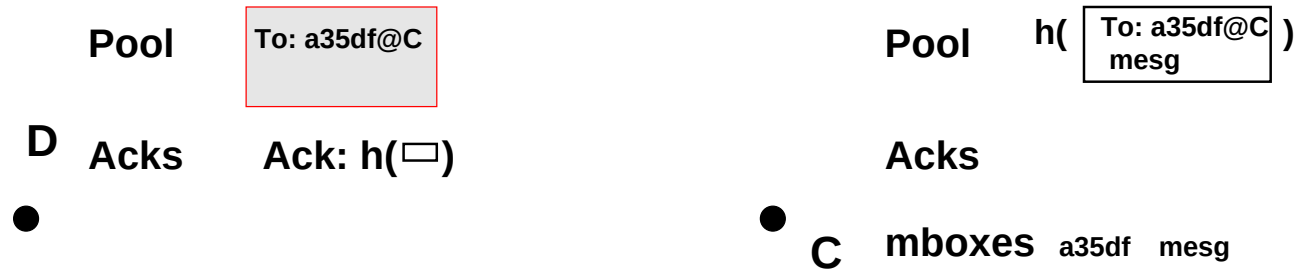
Das Protokoll in Schritten



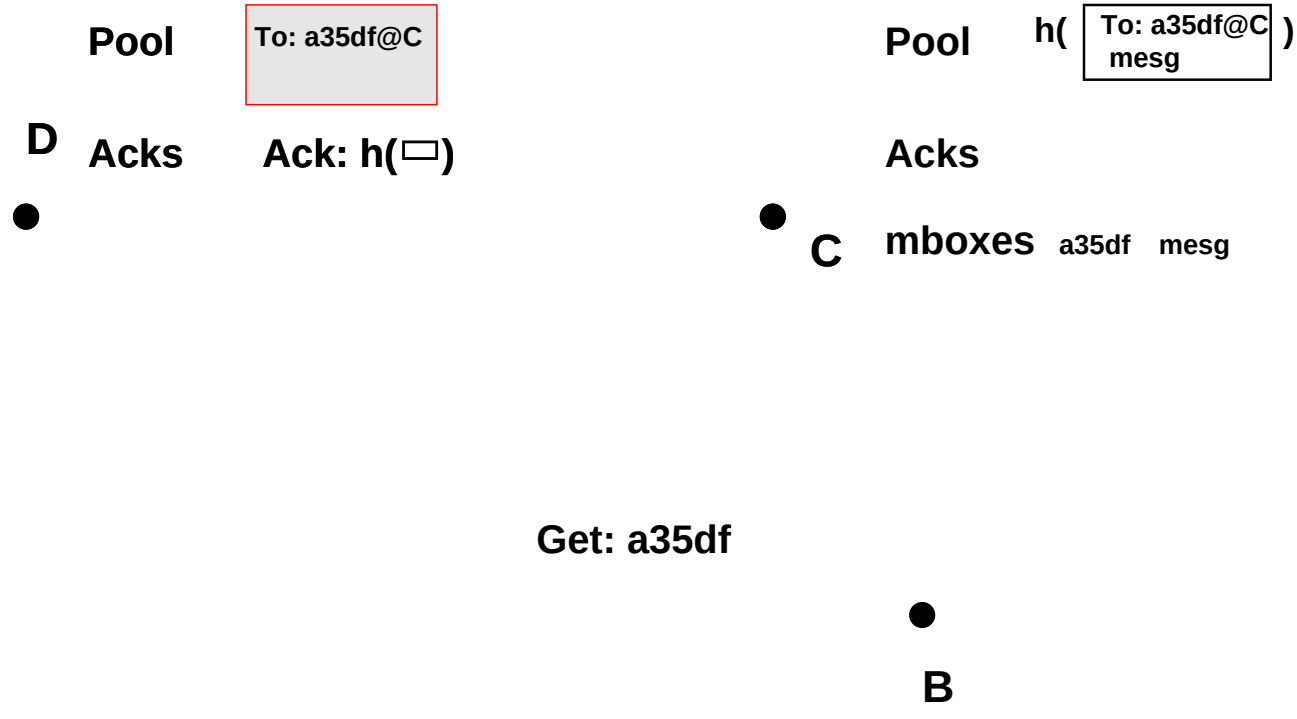
Das Protokoll in Schritten



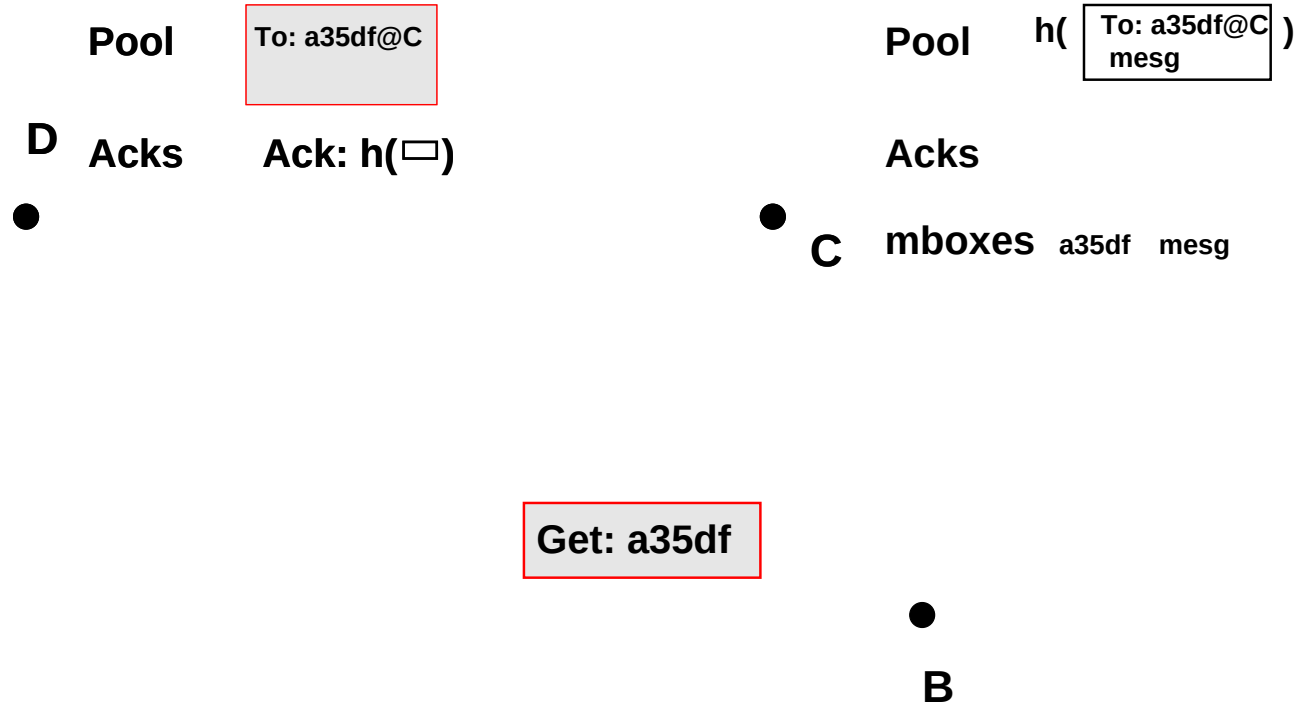
Das Protokoll in Schritten



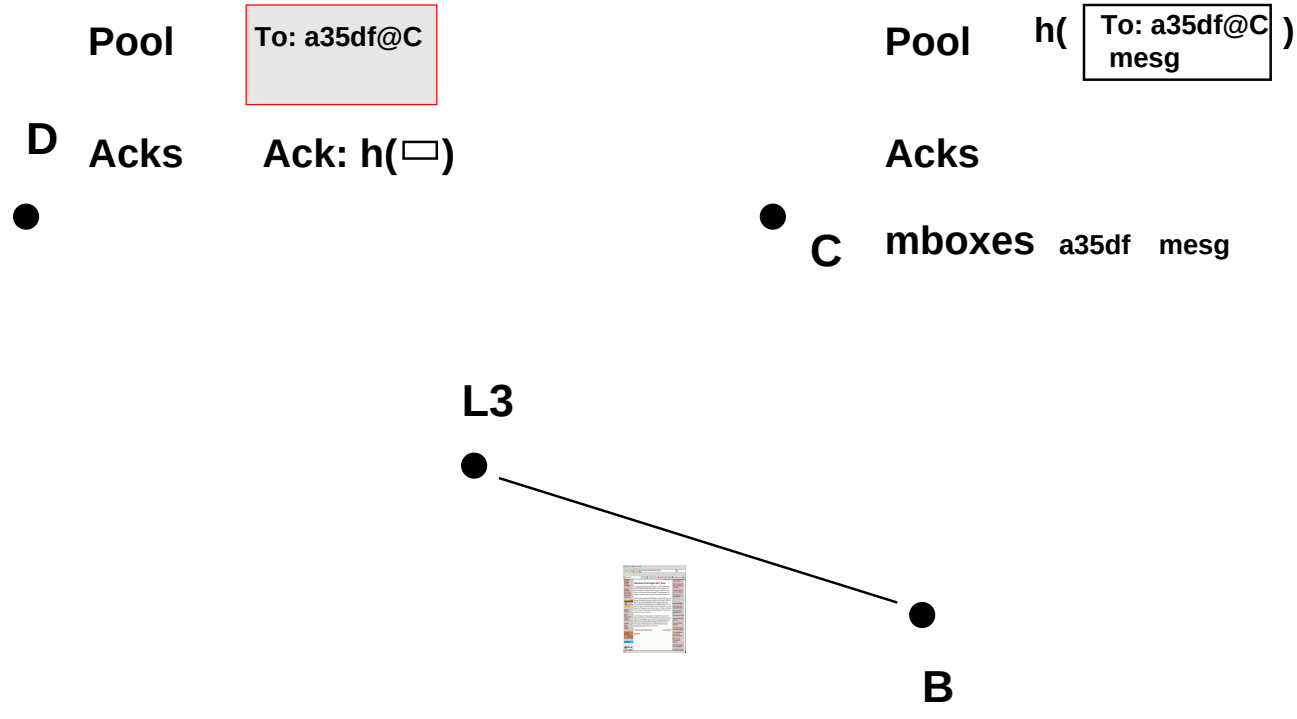
Das Protokoll in Schritten



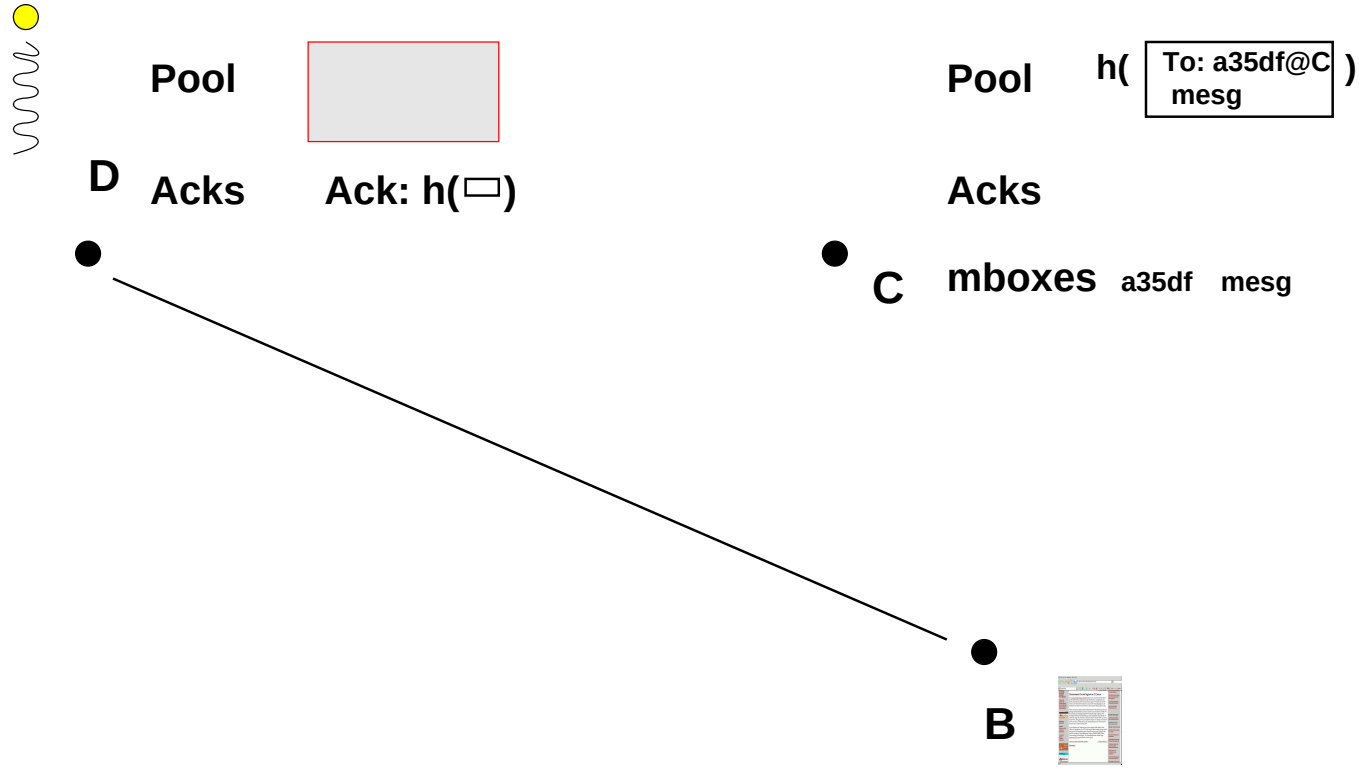
Das Protokoll in Schritten



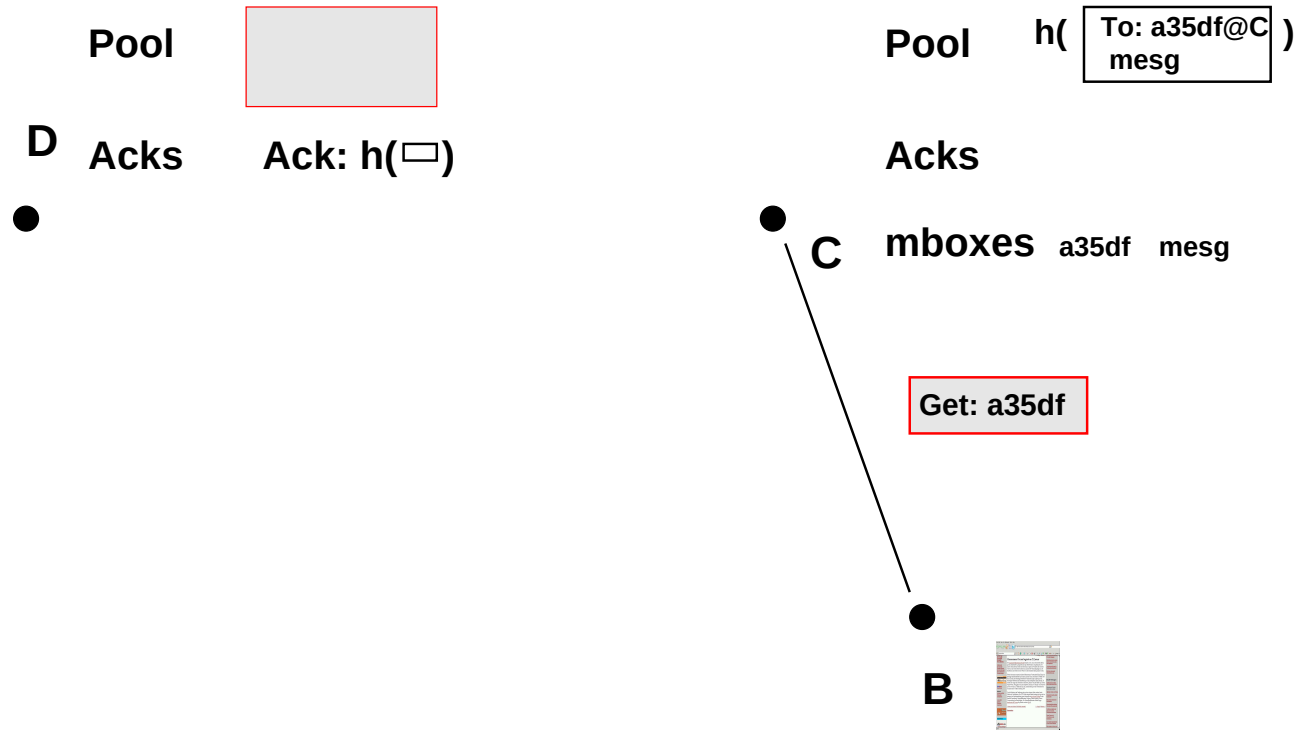
Das Protokoll in Schritten



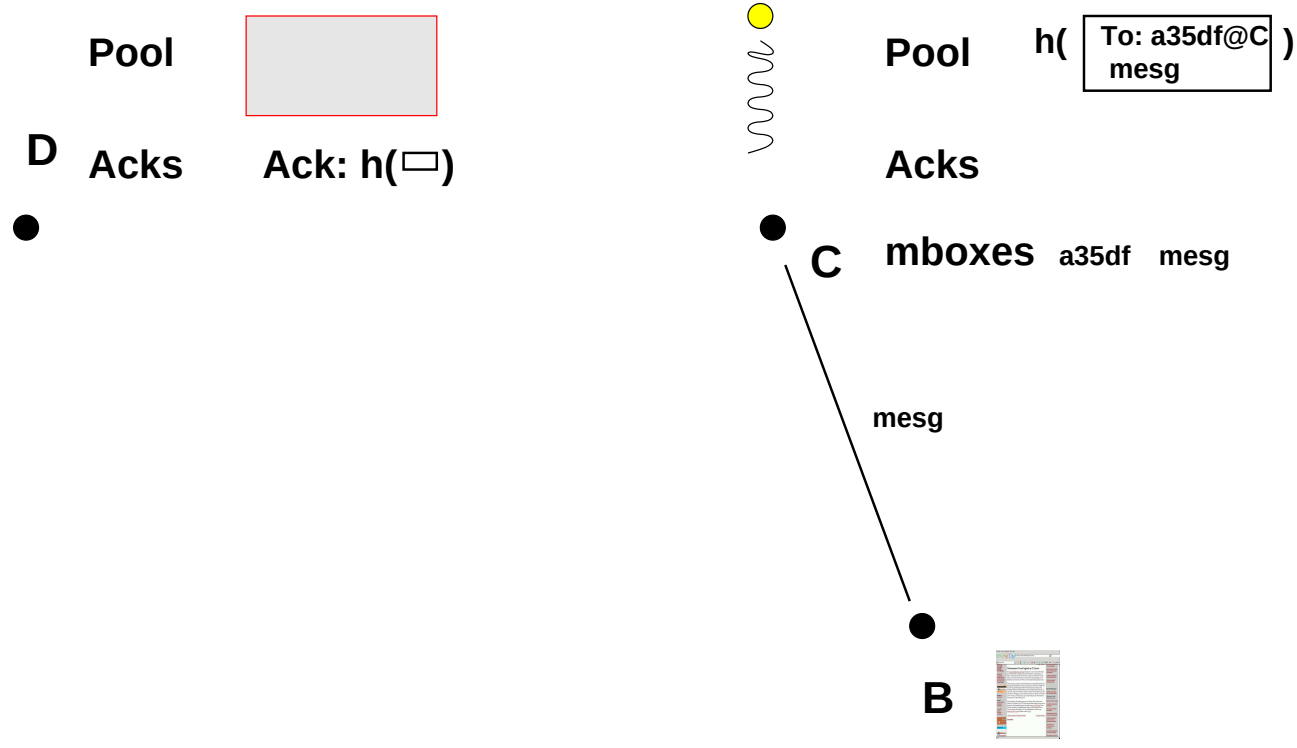
Das Protokoll in Schritten



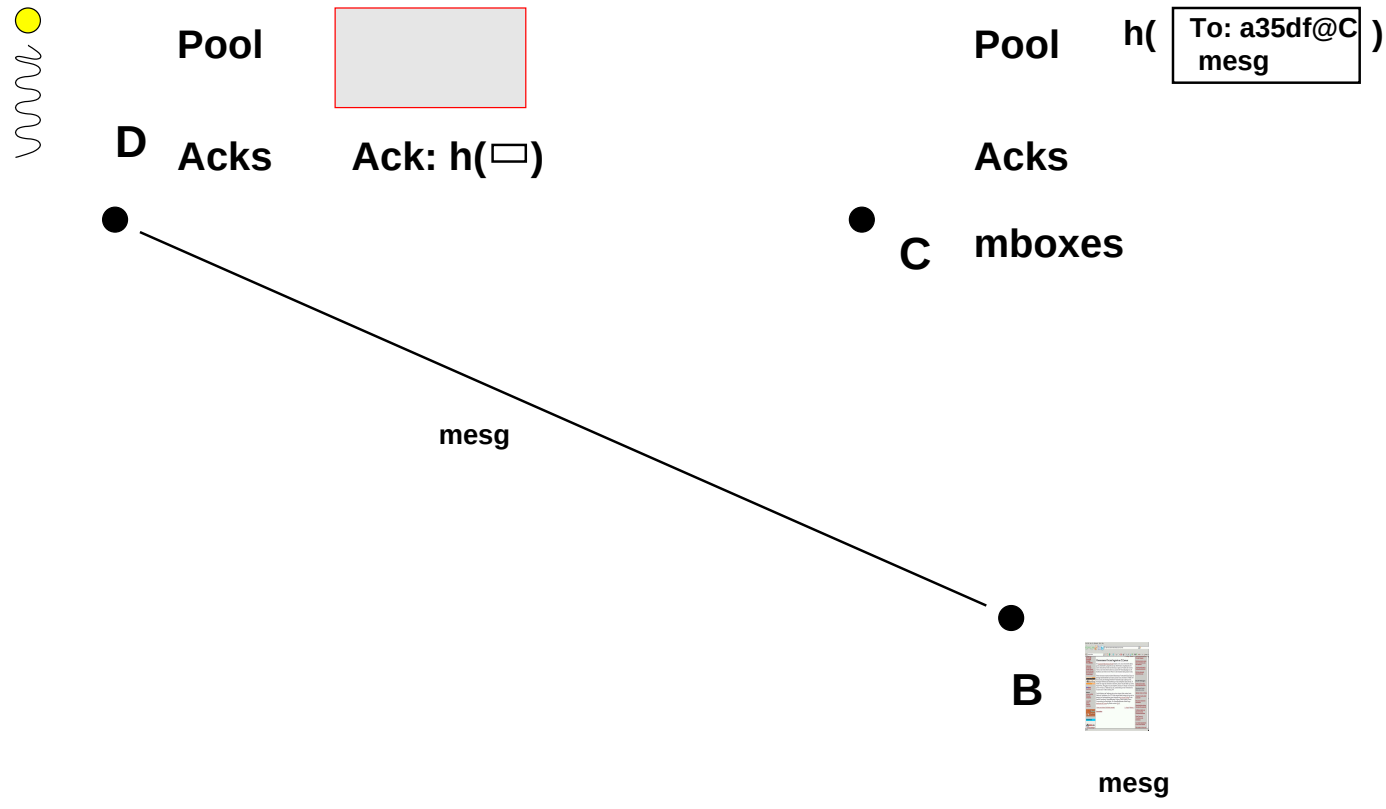
Das Protokoll in Schritten



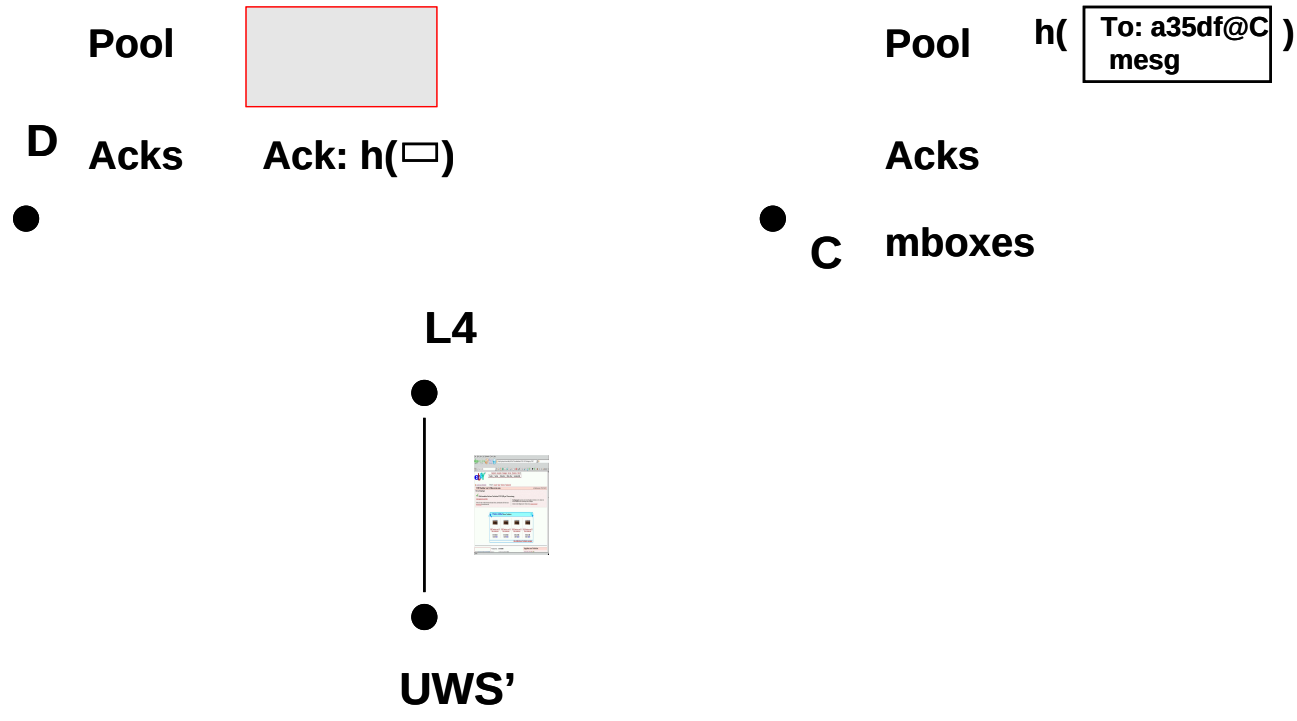
Das Protokoll in Schritten



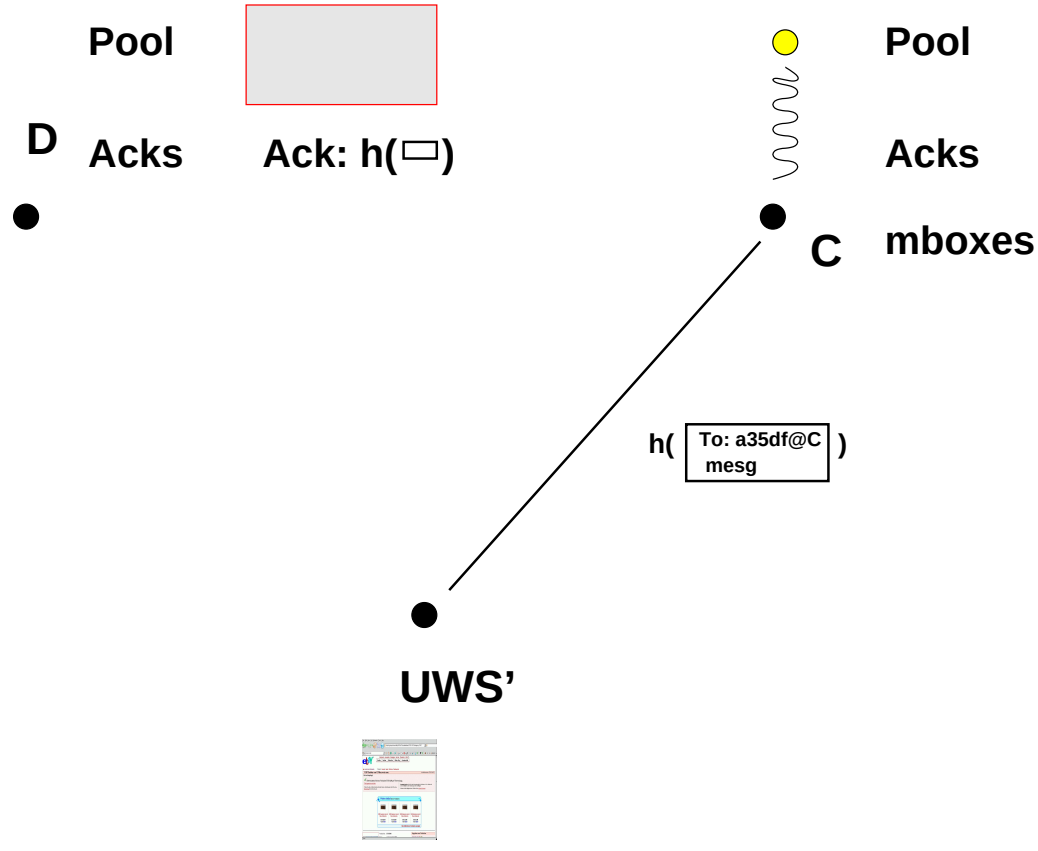
Das Protokoll in Schritten



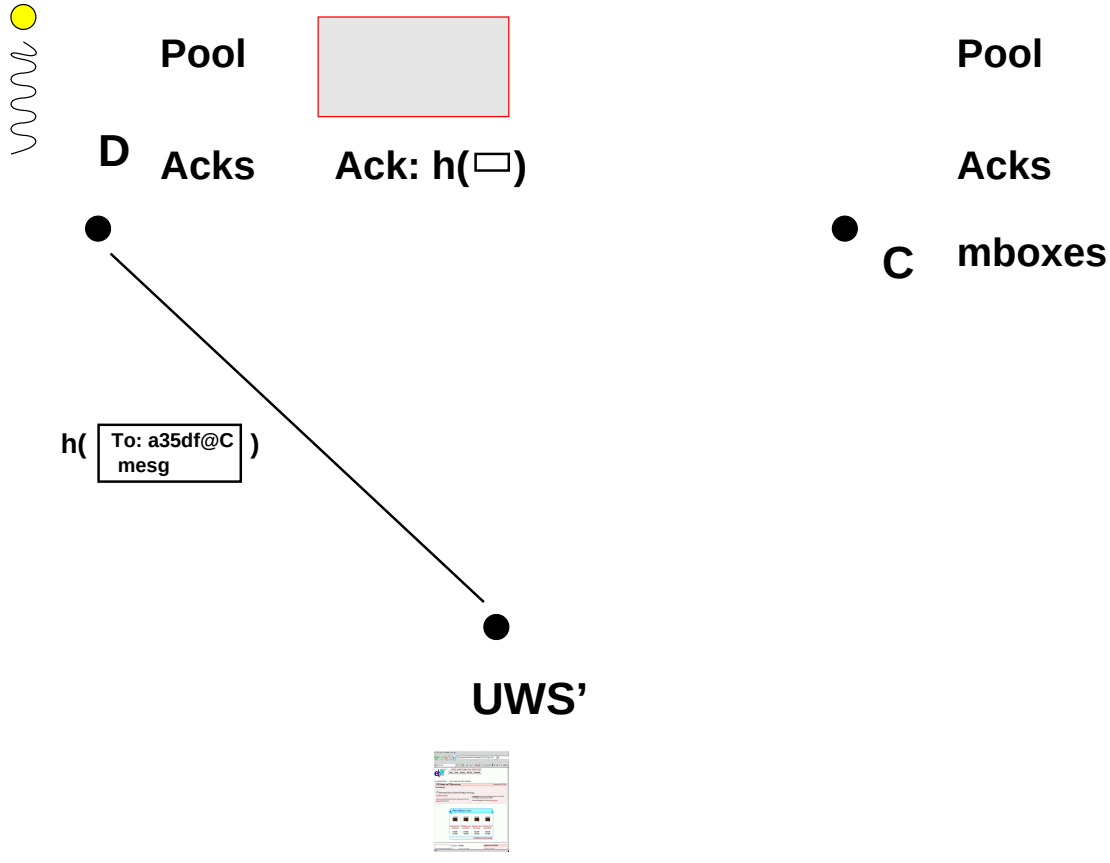
Das Protokoll in Schritten



Das Protokoll in Schritten



Das Protokoll in Schritten



Das Protokoll in Schritten

The End