Anonyme Netzwerke
(TOR-Auszug)

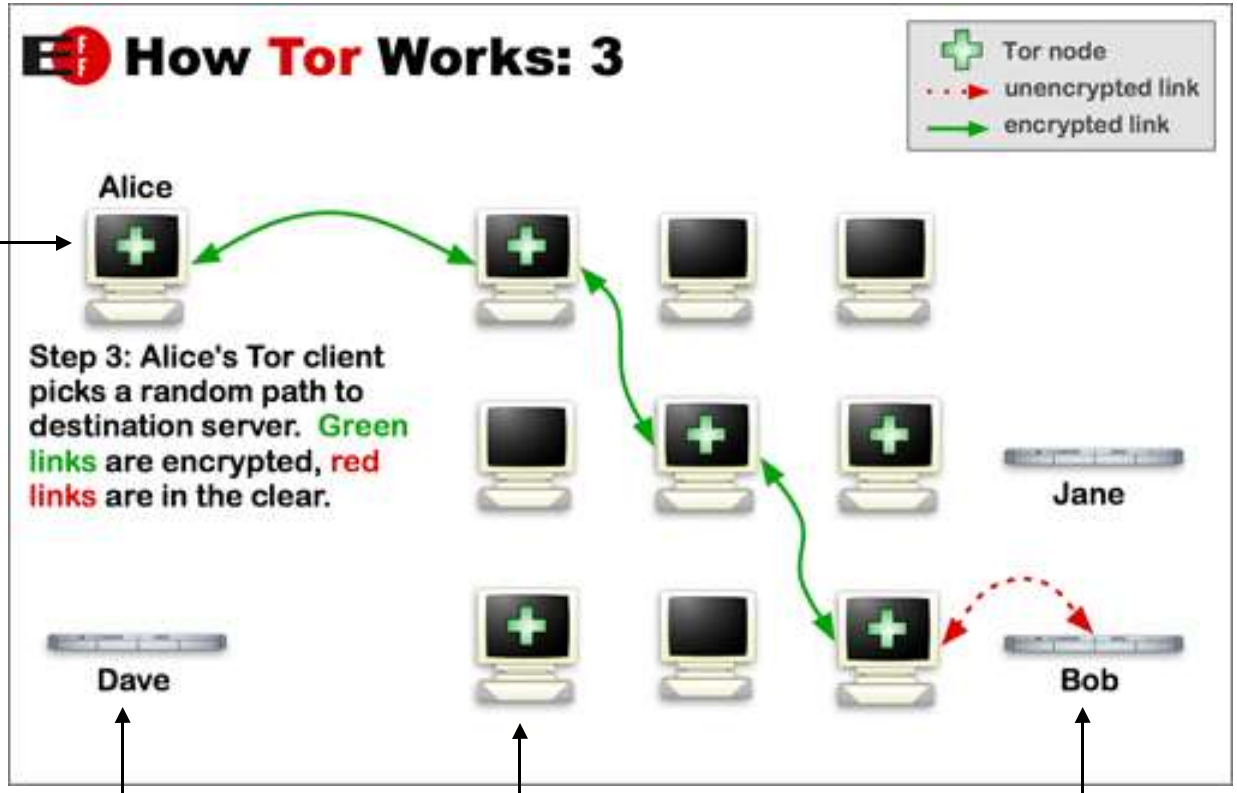
Only criminals have privacy right now;
we need to fix that

Katrin Apel, Alexander Altmann

Was ist Tor?

- Verbindungsorientierter, anonymisierender Kommunikationsdienst
- auf TCP aufsetzendes Netzwerk
- als Server (Onion Router) oder Client (Onion Proxy) installierbar
- Benutzt SOCKS-Proxy-Interface
- Liste der Onion Router: http://serifos.eecs.harvard.edu:8000/cgi-bin/exit.pl

Tor Funktionsprinzip



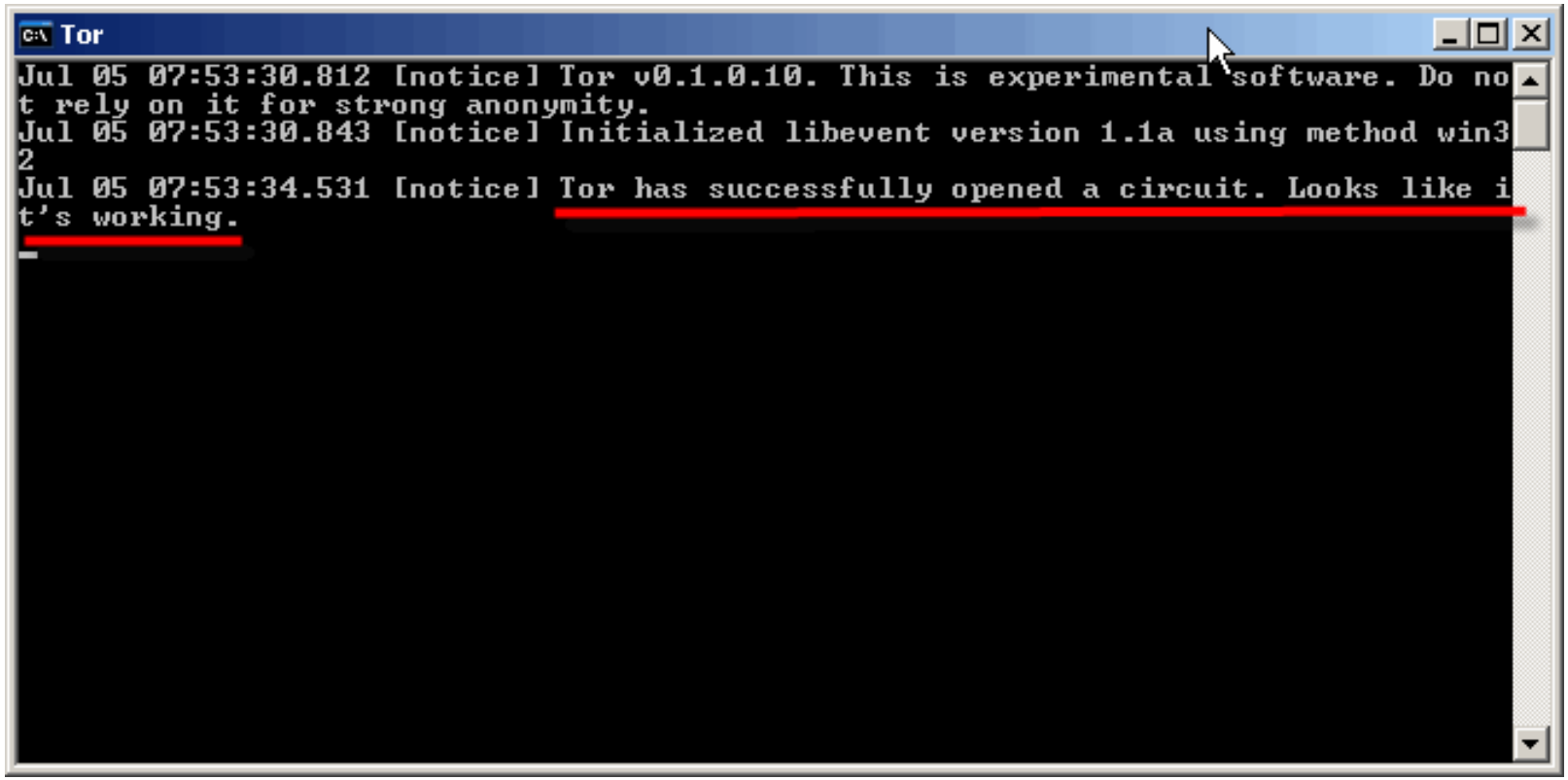
Onion Proxy

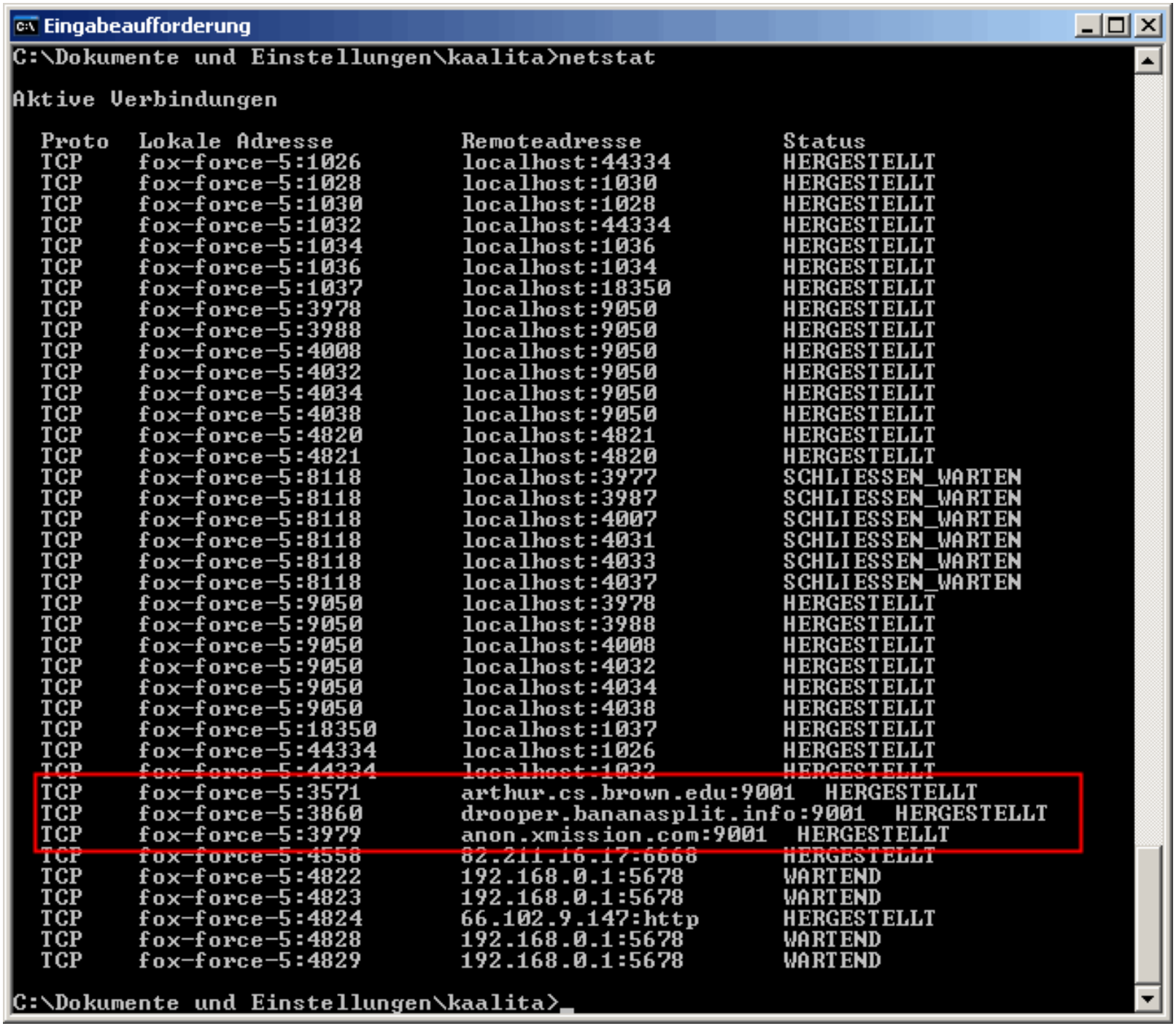
Directory Server

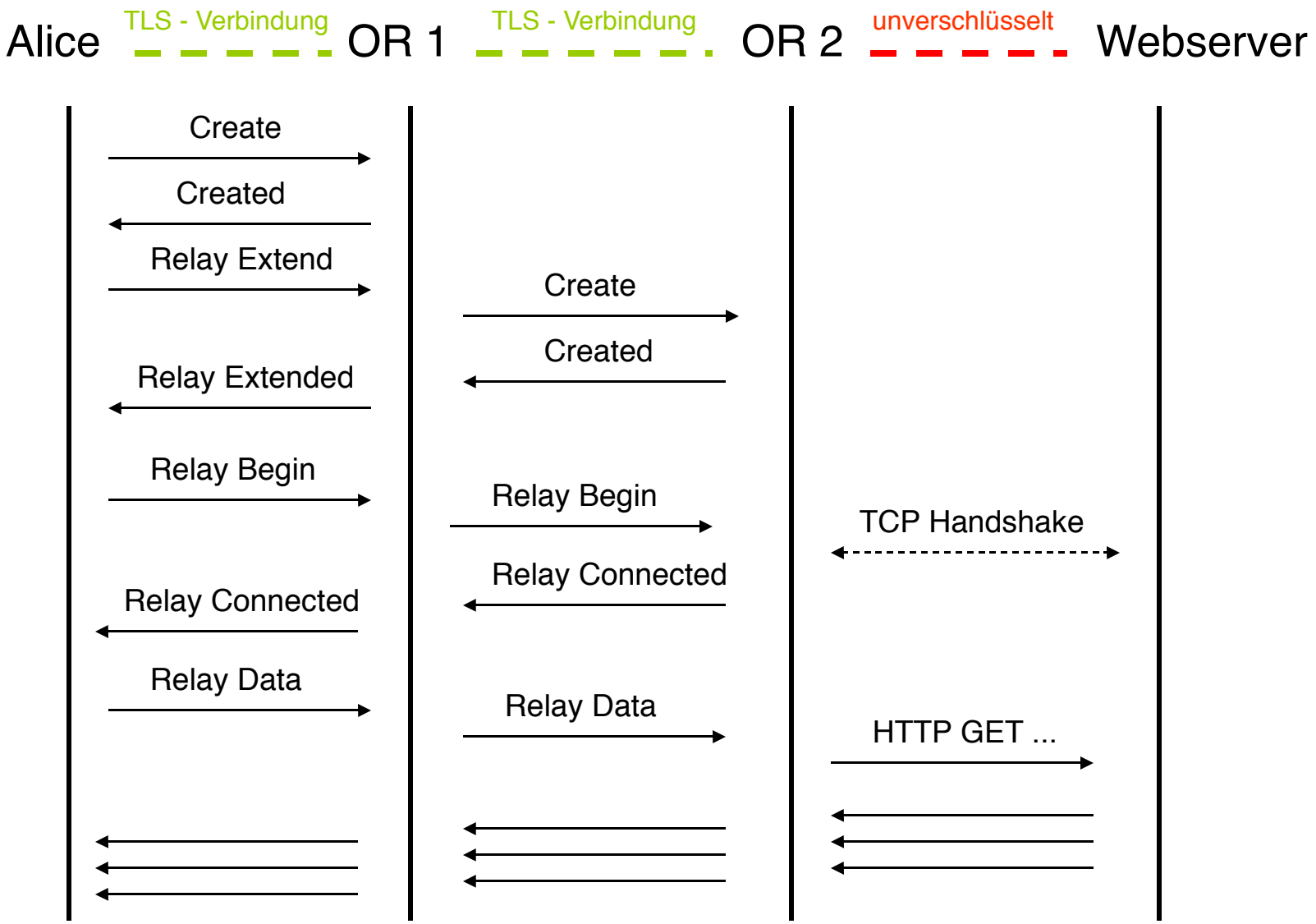
Onion Router

Webserver

Tor - Starten


Tor
Jul 05 07:53:30.812 [notice] Tor v0.1.0.10. This is experimental software. Do not rely on it for strong anonymity.
Jul 05 07:53:30.843 [notice] Initialized libevent version 1.1a using method win32
Jul 05 07:53:34.531 [notice] Tor has successfully opened a circuit. Looks like it's working.

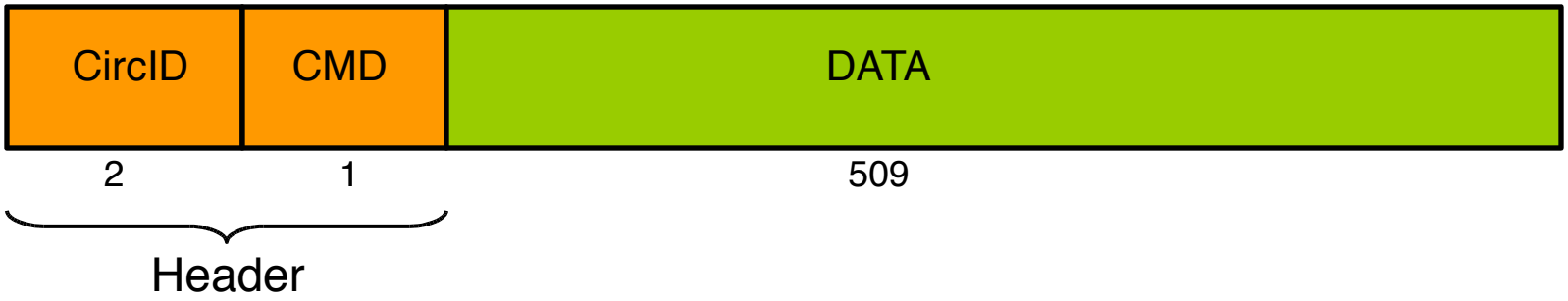

Eingabeaufforderung
C:\Dokumente und Einstellungen\kaalita>netstat
Aktive Verbindungen
Proto Lokale Adresse Remoteadresse Status
TCP fox-force-5:1026 localhost:44334 HERGESTELLT
TCP fox-force-5:1028 localhost:1030 HERGESTELLT
TCP fox-force-5:1030 localhost:1028 HERGESTELLT
TCP fox-force-5:1032 localhost:44334 HERGESTELLT
TCP fox-force-5:1034 localhost:1036 HERGESTELLT
TCP fox-force-5:1036 localhost:1034 HERGESTELLT
TCP fox-force-5:1037 localhost:18350 HERGESTELLT
TCP fox-force-5:3978 localhost:9050 HERGESTELLT
TCP fox-force-5:3988 localhost:9050 HERGESTELLT
TCP fox-force-5:4008 localhost:9050 HERGESTELLT
TCP fox-force-5:4032 localhost:9050 HERGESTELLT
TCP fox-force-5:4034 localhost:9050 HERGESTELLT
TCP fox-force-5:4038 localhost:9050 HERGESTELLT
TCP fox-force-5:4820 localhost:4821 HERGESTELLT
TCP fox-force-5:4821 localhost:4820 HERGESTELLT
TCP fox-force-5:8118 localhost:3977 SCHLIESSEN_WARTEN
TCP fox-force-5:8118 localhost:3987 SCHLIESSEN_WARTEN
TCP fox-force-5:8118 localhost:4007 SCHLIESSEN_WARTEN
TCP fox-force-5:8118 localhost:4031 SCHLIESSEN_WARTEN
TCP fox-force-5:8118 localhost:4033 SCHLIESSEN_WARTEN
TCP fox-force-5:8118 localhost:4037 SCHLIESSEN_WARTEN
TCP fox-force-5:9050 localhost:3978 HERGESTELLT
TCP fox-force-5:9050 localhost:3988 HERGESTELLT
TCP fox-force-5:9050 localhost:4008 HERGESTELLT
TCP fox-force-5:9050 localhost:4032 HERGESTELLT
TCP fox-force-5:9050 localhost:4034 HERGESTELLT
TCP fox-force-5:9050 localhost:4038 HERGESTELLT
TCP fox-force-5:18350 localhost:1037 HERGESTELLT
TCP fox-force-5:44334 localhost:1026 HERGESTELLT
TCP fox-force-5:44334 localhost:1032 HERGESTELLT
TCP fox-force-5:3571 arthur.cs.brown.edu:9001 HERGESTELLT
TCP fox-force-5:3860 drooper.bananasplit.info:9001 HERGESTELLT
TCP fox-force-5:3979 anon.xmission.com:9001 HERGESTELLT
TCP fox-force-5:4558 82.211.16.17:6668 HERGESTELLT
TCP fox-force-5:4822 192.168.0.1:5678 WARTEND
TCP fox-force-5:4823 192.168.0.1:5678 WARTEND
TCP fox-force-5:4824 66.102.9.147:http HERGESTELLT
TCP fox-force-5:4828 192.168.0.1:5678 WARTEND
TCP fox-force-5:4829 192.168.0.1:5678 WARTEND
C:\Dokumente und Einstellungen\kaalita>


Alice
TLS - Verbindung
OR 1
TLS - Verbindung
OR 2
unverschlüsselt
Webserver
Create
Created
Relay Extend
Create
Created
Relay Extended
Relay Begin
Relay Begin
TCP Handshake
Relay Connected
Relay Connected
Relay Data
Relay Data
HTTP GET ...

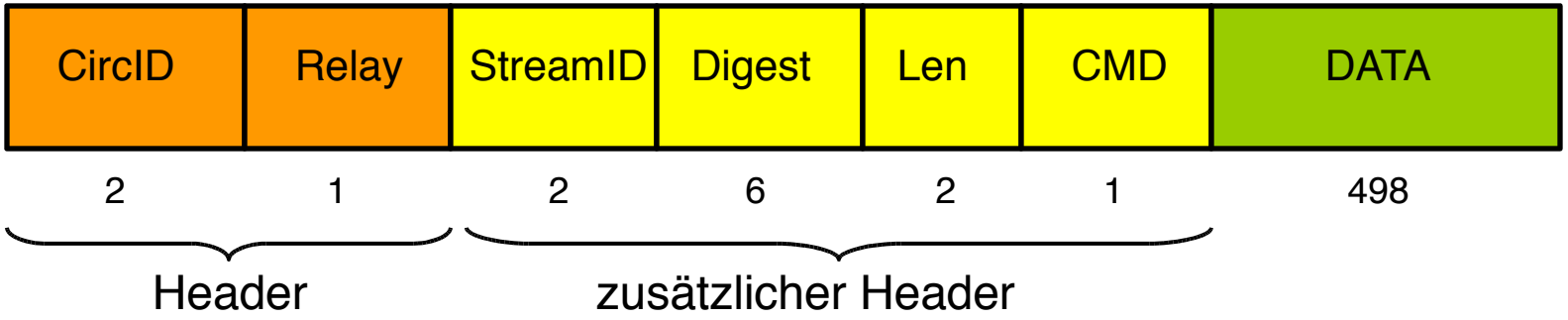
Tor – Zellen

Zellen fester Größe

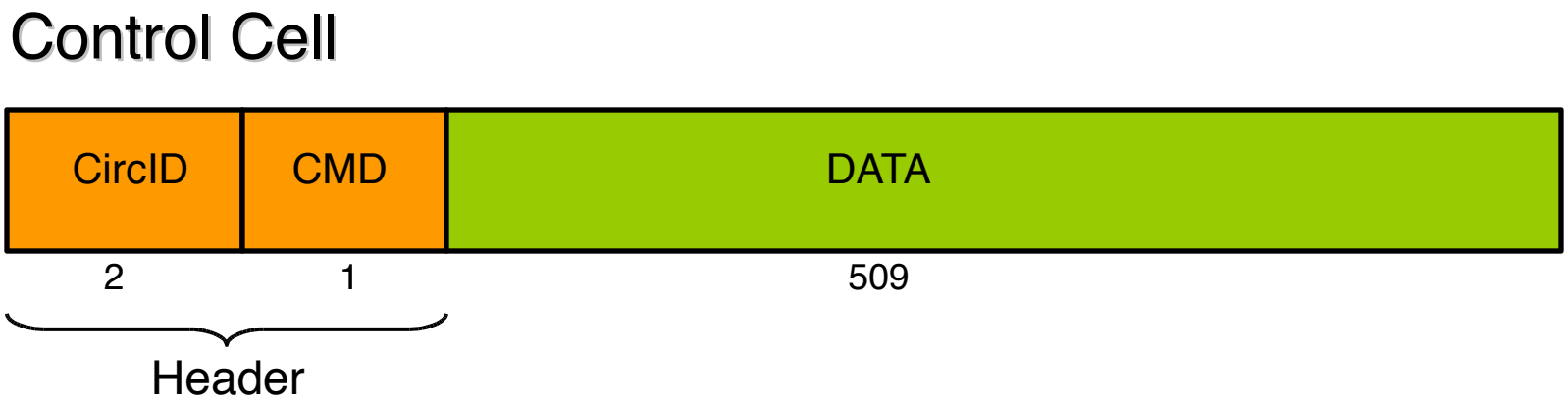
Control Cell



Relay Cell



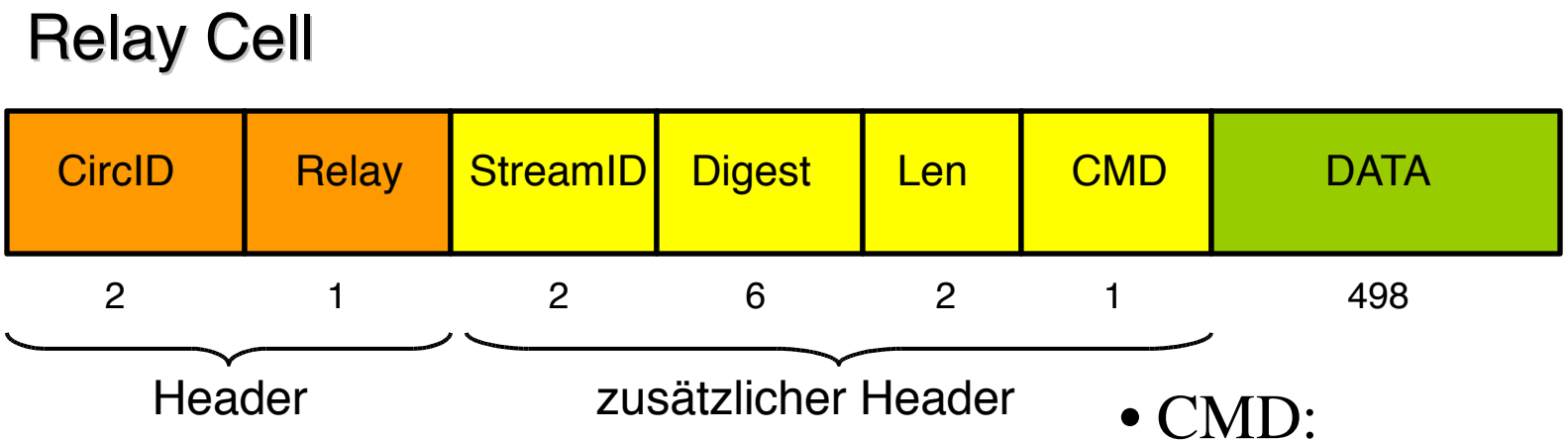
Control Cell



Control Zellen werden immer vom empfangenden Knoten direkt interpretiert

- CMD:
  - Create / Created
  - Padding
  - Destroy

Relay Cell



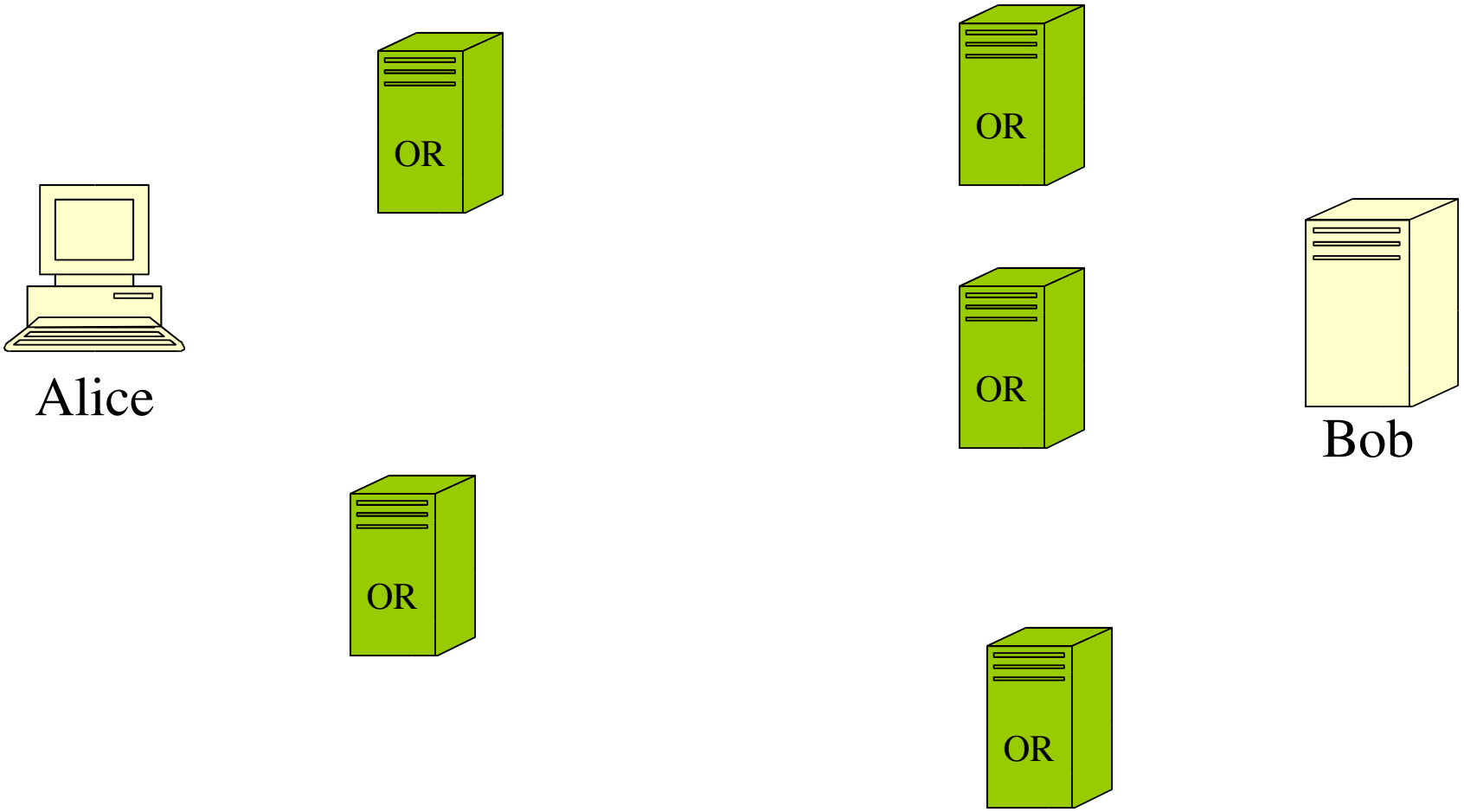
Übermitteln End-To-End Stream Daten

- CMD:
  - Relay data
  - Relay begin
  - Relay end
  - Relay Teardown
  - Relay Connected
  - Relay Extended
  - Relay Truncated
  - Relay Sendme
  - Relay Drop

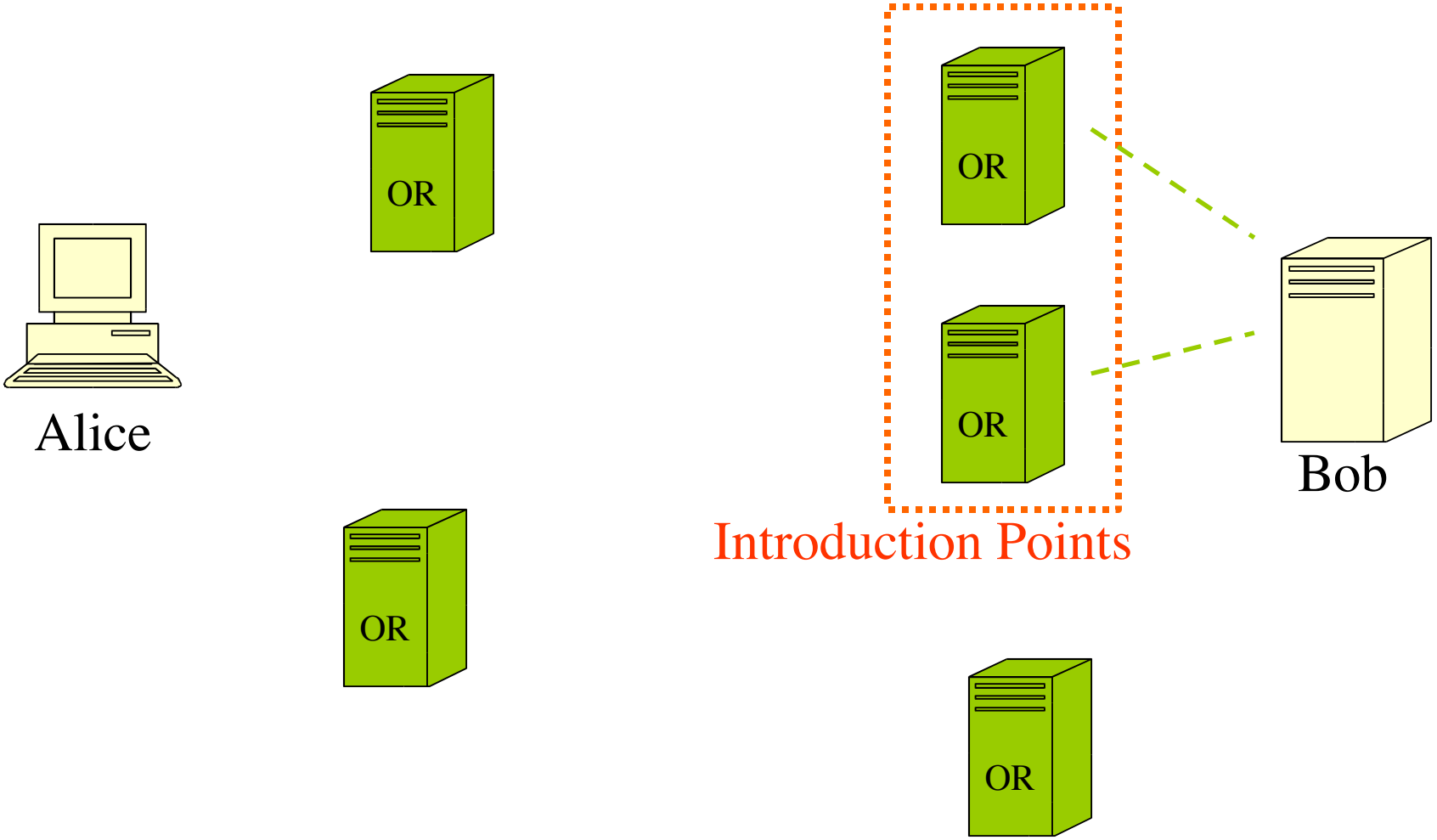
Tor Hidden Services

- Anonyme Webserver betreiben
- .onion Top Level Domain
- Location Hidden Tor Wiki
  http://6sxoyfb3h2nvok2d.onion/tor/
- Rendezvous Points

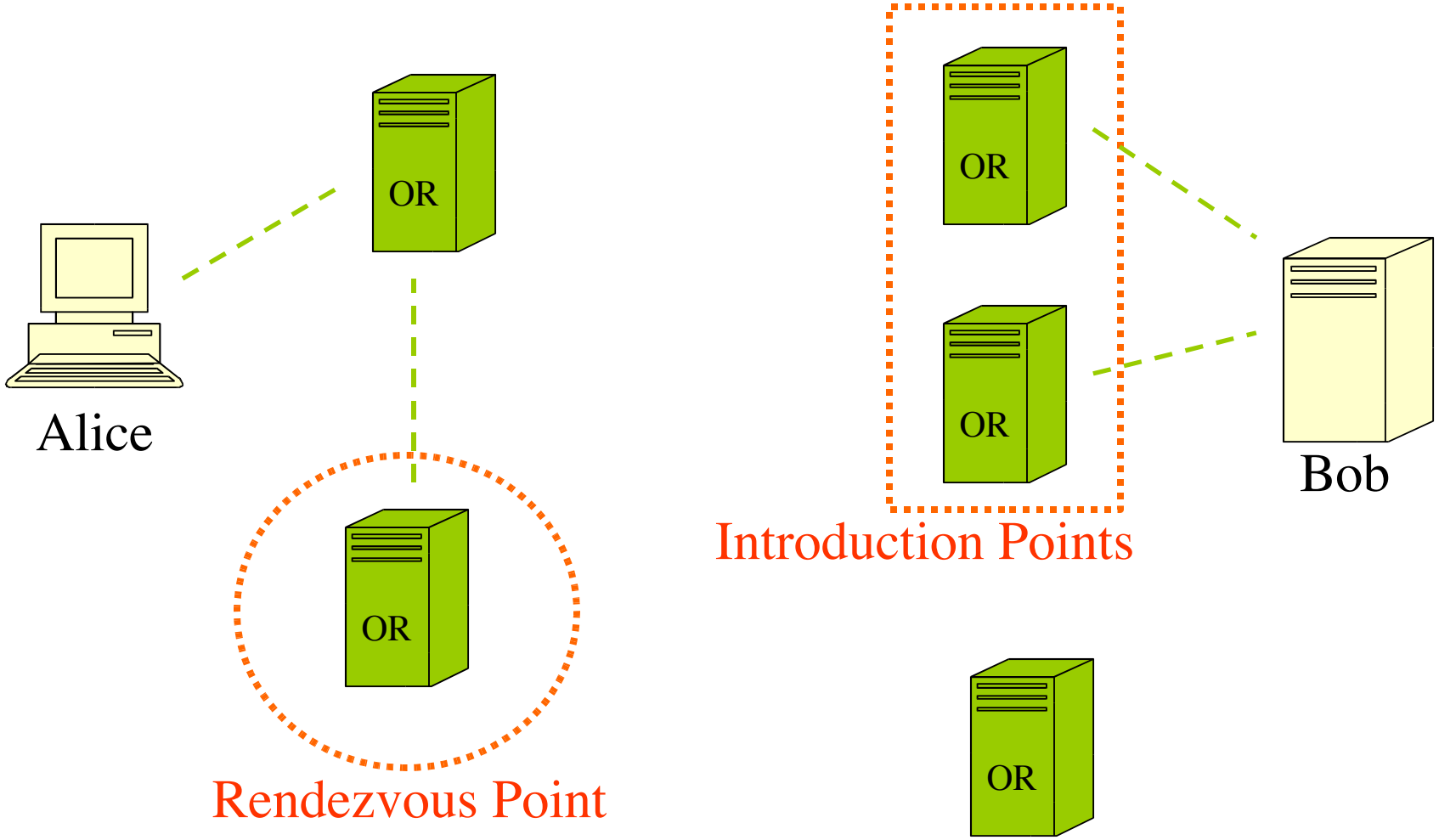
Tor Hidden Services



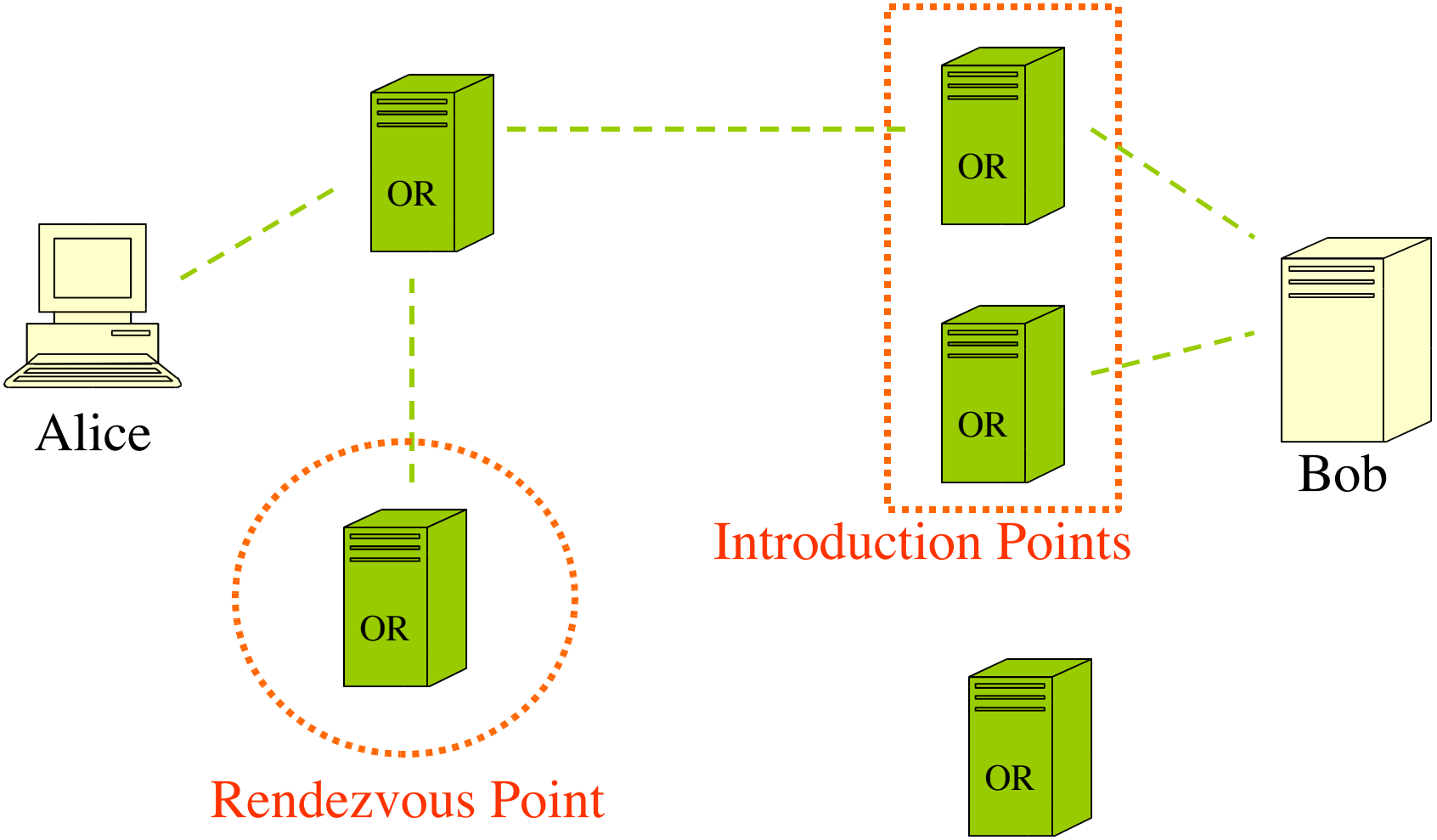
Tor Hidden Services



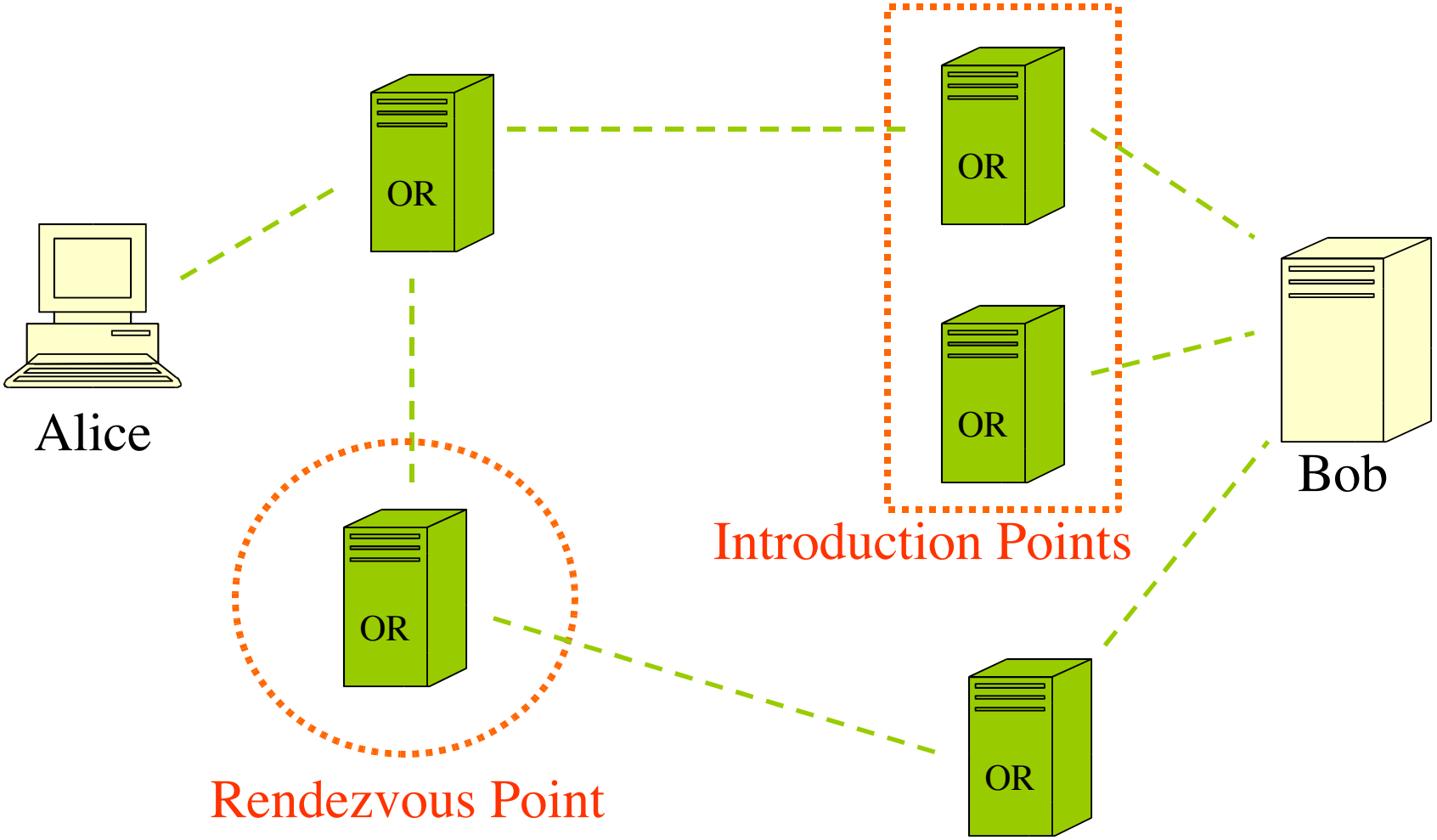
Tor Hidden Services



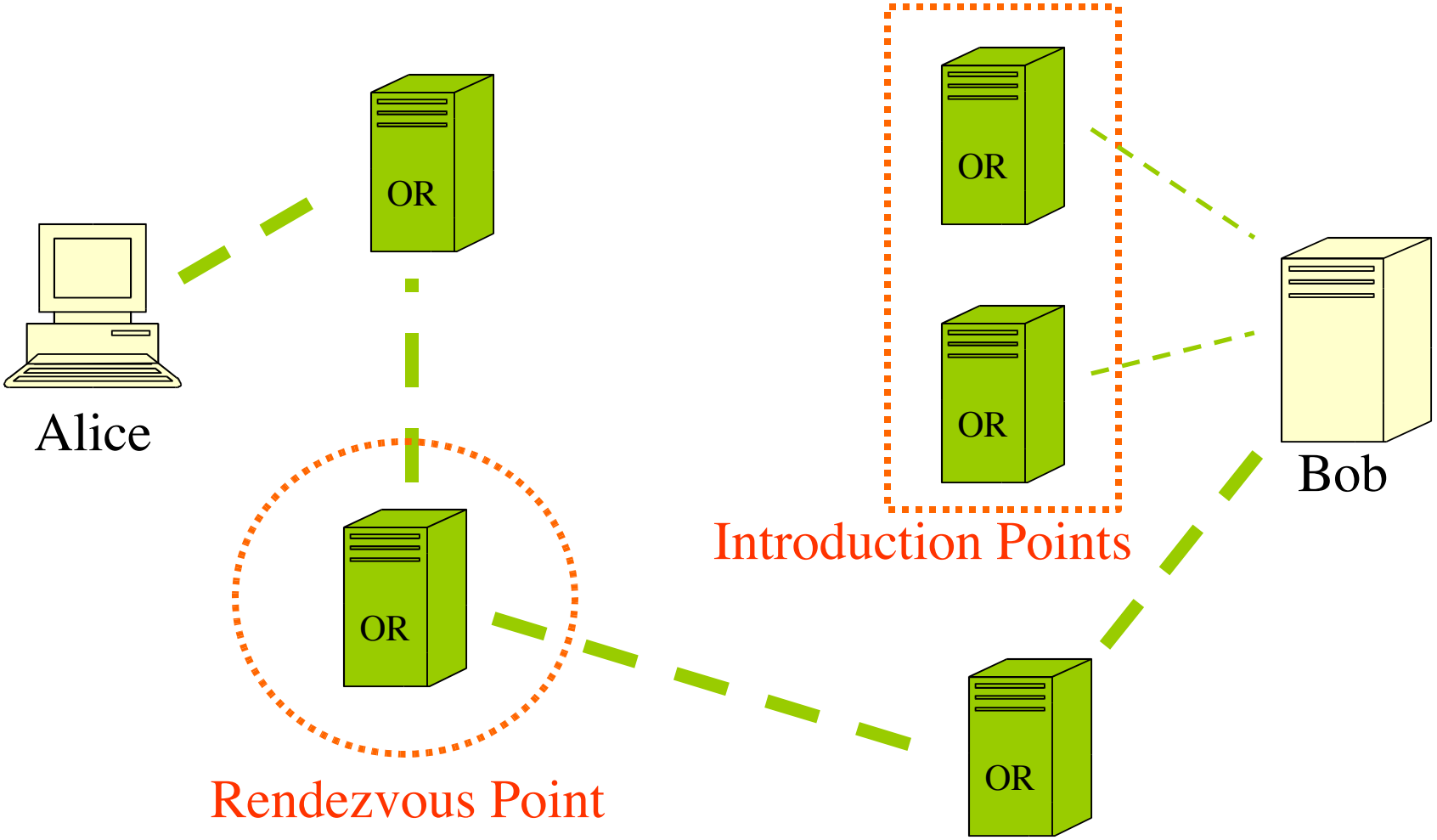
Tor Hidden Services



Tor Hidden Services



Tor Hidden Services



Tor - Performance

- Verlangsamung deutlich, aber Surfen und Chatten noch gut möglich
- Sehr starke Schwankungen
- Hängt manchmal komplett
- Beispiel: Dateigröße 32.3 MB
  - Ohne Tor: 4:29min
  - Mit Tor: 6:10min

Tor – Fazit

- Vorteile
  - sehr einfache Installation/Bedienung
  - Für Win32, Linux und MacOS X verfügbar
  - SOCKS Proxy Interface
  - Missbrauchsschutz (Exit Policies, DDoS, Spam)
  - Guter Kompromiß
- Nachteile
  - Performanz
  - Exit Server Problem
  - Google Problem
  - IRC Problem
  - Wikipedia Problem
  - Email Blacklist

Quellen

- Tor http://tor.eff.org/
- Liste der Onion Router http://www.noreply.org/tor-running-routers/
- Onion Router Statistiken http://serifos.eecs.harvard.edu:8000/cgi-bin/exit.pl
- Privoxy: http://www.privoxy.org/