AN.ON
NEXT GENERATION

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

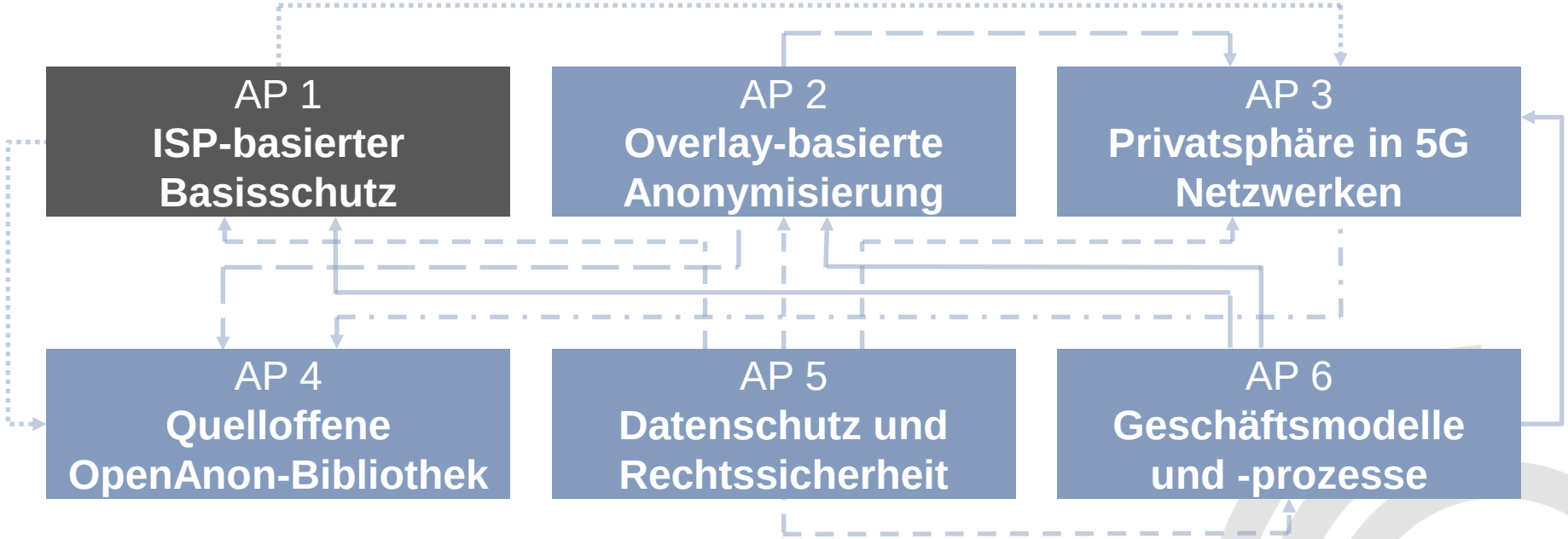
Privatsphäre als inhärente Eigenschaft eines Kommunikationsnetzes

Matthias Marx

Universität Hamburg – Sicherheit in verteilten Systemen

AN.ON-Next

Anonymität Online der nächsten Generation



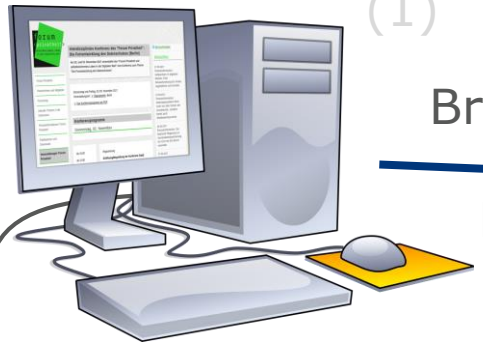
Arbeitspaket 1

- Tracking-Basisschutz für alle Nutzer
- Verlagerung des Schutzes zum vertrauenswürdigen Internetprovider
- Nutzeranfragen erscheinen ggü. Diensten mit unterschiedlichen Identitäten

Tracking

Anwendungsebene

(1)



Browser Fingerprint

Referer

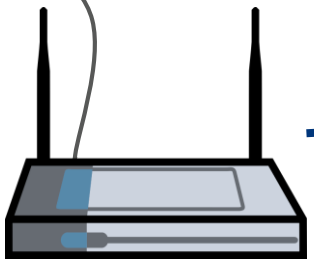
Cookies

Tracker

(3)

Profile

(4)



IP-Adresse

(2)

Netzwerkebene

Tracking

Anwendungsebene

Browser Fingerprint

Referer

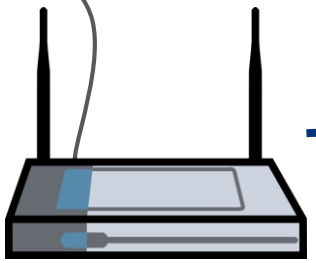
Cookies

AdBlock
NoScript

(5)

Tracker

Profile



IP-Adresse

VPNs
Tor
JAP

Netzwerkebene

Tracking

Anwendungsebene

Browser Fingerprint

Referer

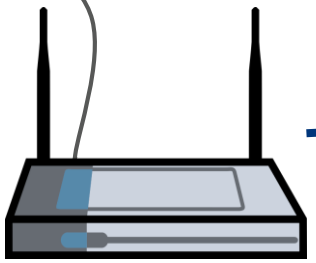
Cookies

AdBlock
NoScript

Tor-
Browser

Tracker

Profile



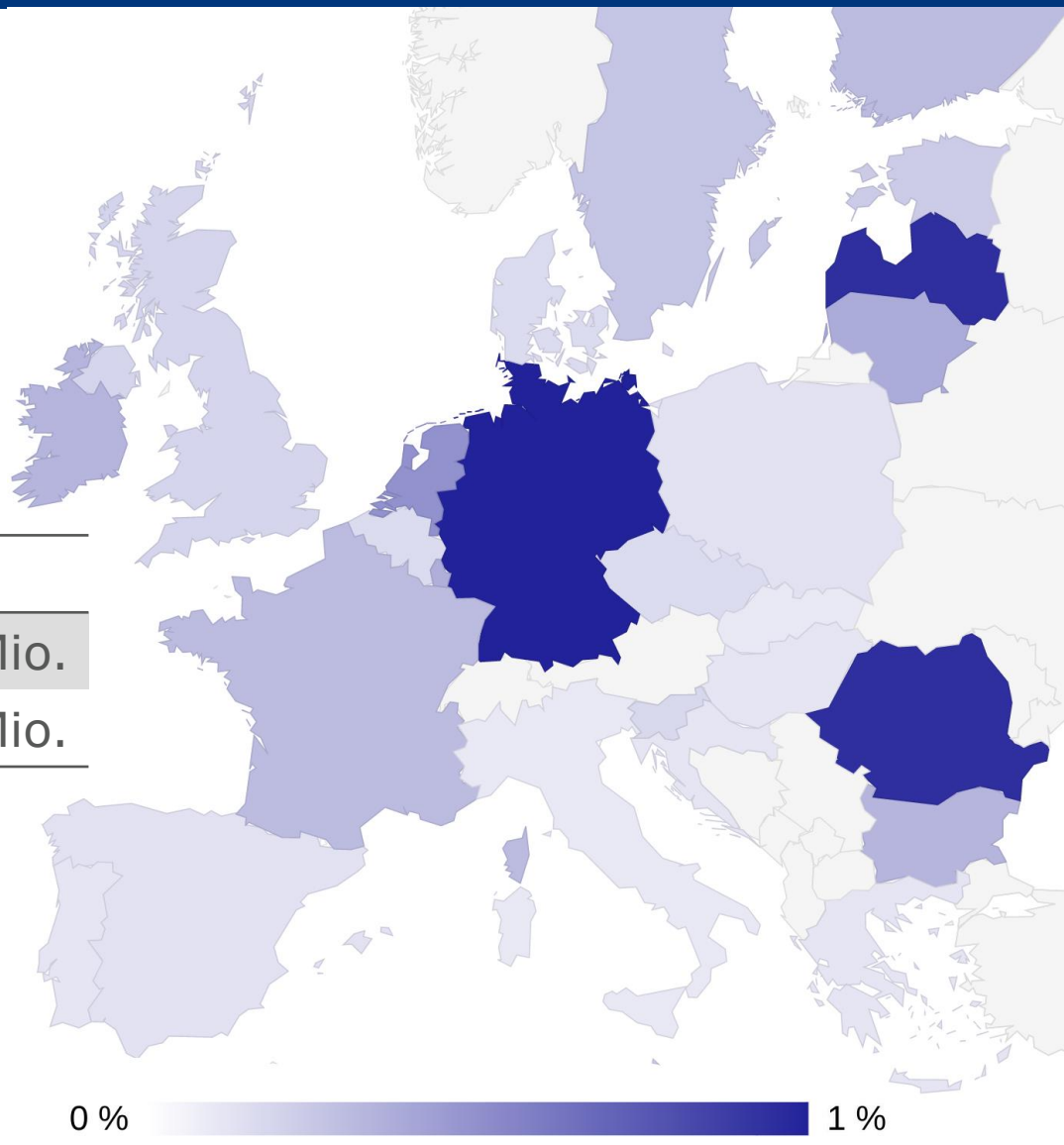
IP-Adresse

VPNs
Tor
JAP

Netzwerkebene

Verbreitung von Tor

Nutzer	Weltweit	EU
Internet	> 3600 Mio.	> 500 Mio.
Tor	2,5 Mio.	1 Mio.



Quelle: Eigenes Werk, basierend auf Daten von Tor Metrics (2017) und ITU (2016)

Herausforderungen

- Existierende Schutzmaßnahmen werden nicht eingesetzt
  - Fehlendes Problembewusstsein
  - Fehlender technischer Sachverstand
- Smarte Geräte können nicht geschützt werden
- Existierende Schutzmaßnahmen reichen nicht aus
  - Werbenetze nutzen IPv4-Adressen und IPv6-Präfixe und -Suffixe um gelöschte Cookies wiederherzustellen
  - Tägliche IP-Adresswechsel schützen nicht vor Profilbildung

Anforderungen

Ziel: Ein leichgewichtiger Anonymisierungsdienst

- Keine Änderungen an Betriebssystem, Software oder Hardware des Nutzers notwendig
- Anonymisierung soll auf Heimrouter oder im Rechenzentrum des ISPs erfolgen
- Anonymisierung soll Nutzererlebnis nicht beeinflussen
  - Keine Unterbrechung von Diensten oder Verbindungen
  - Keine wahrnehmbarer Zunahme der Latenz

Lösungsvorschlag 1

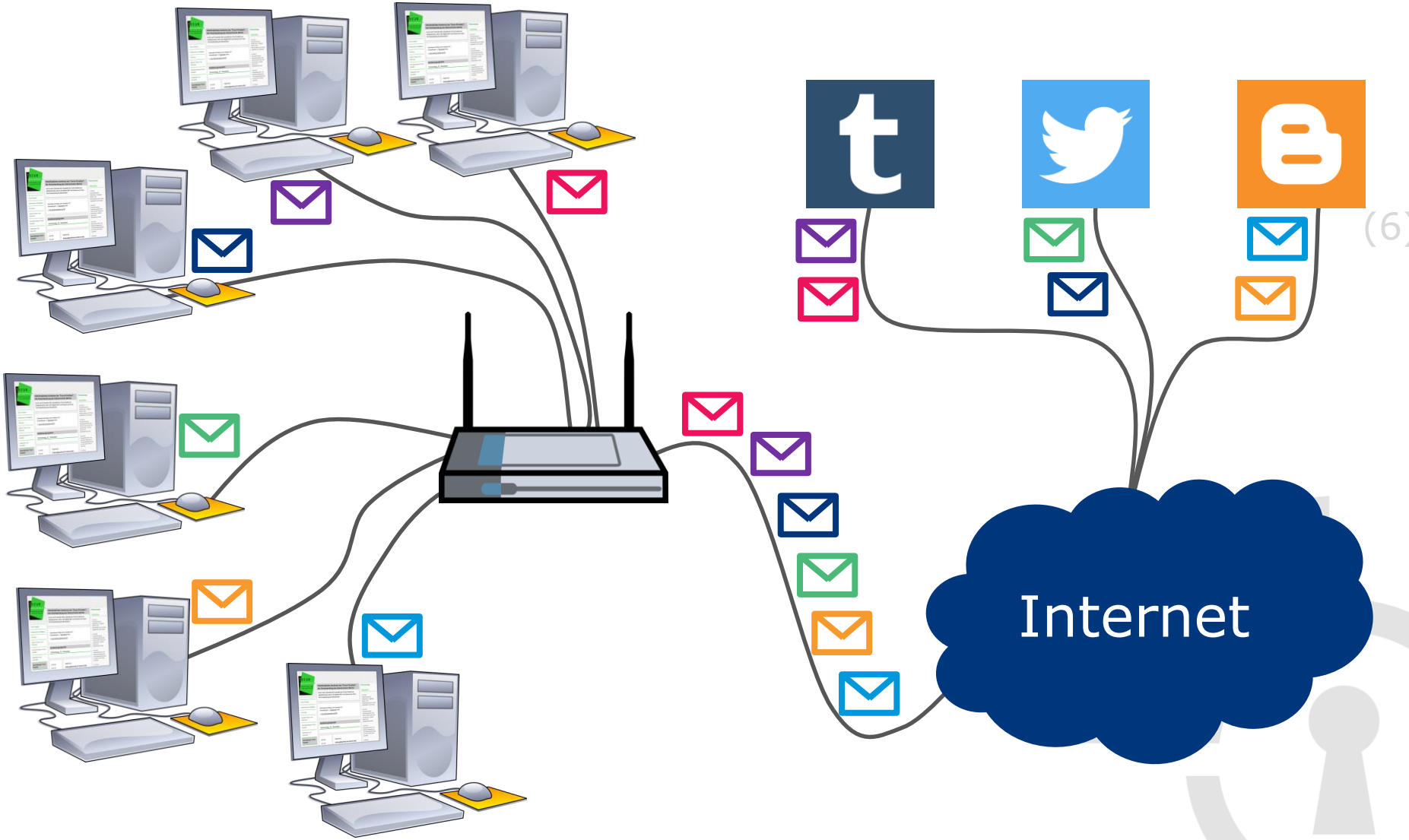
Address Sharing

Mehrere Nutzer teilen sich eine IP-Adresse

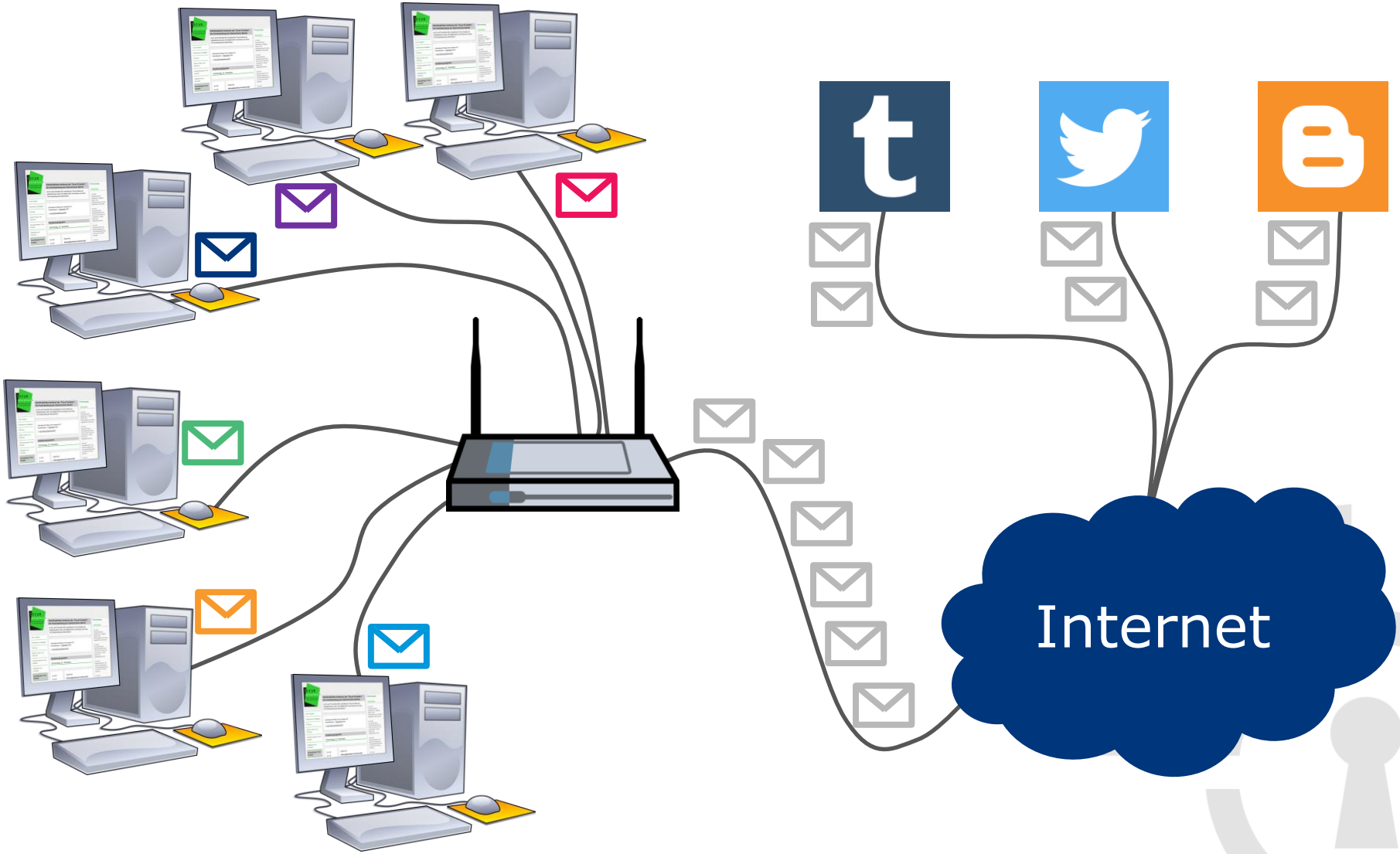
- Nutzer mit gleicher IP-Adresse bilden eine Anonymitätsmenge
- Tracker können Nutzer nicht mehr anhand ihrer IP-Adresse unterscheiden

- Network Address Translation (NAT) wird seit Jahrzehnten genutzt
  - Ermöglicht sparsamen Umgang mit knappen IPv4-Adressen
  - NAT ist auch für IPv6 möglich

Address Sharing - Architektur



Address Sharing - Architektur



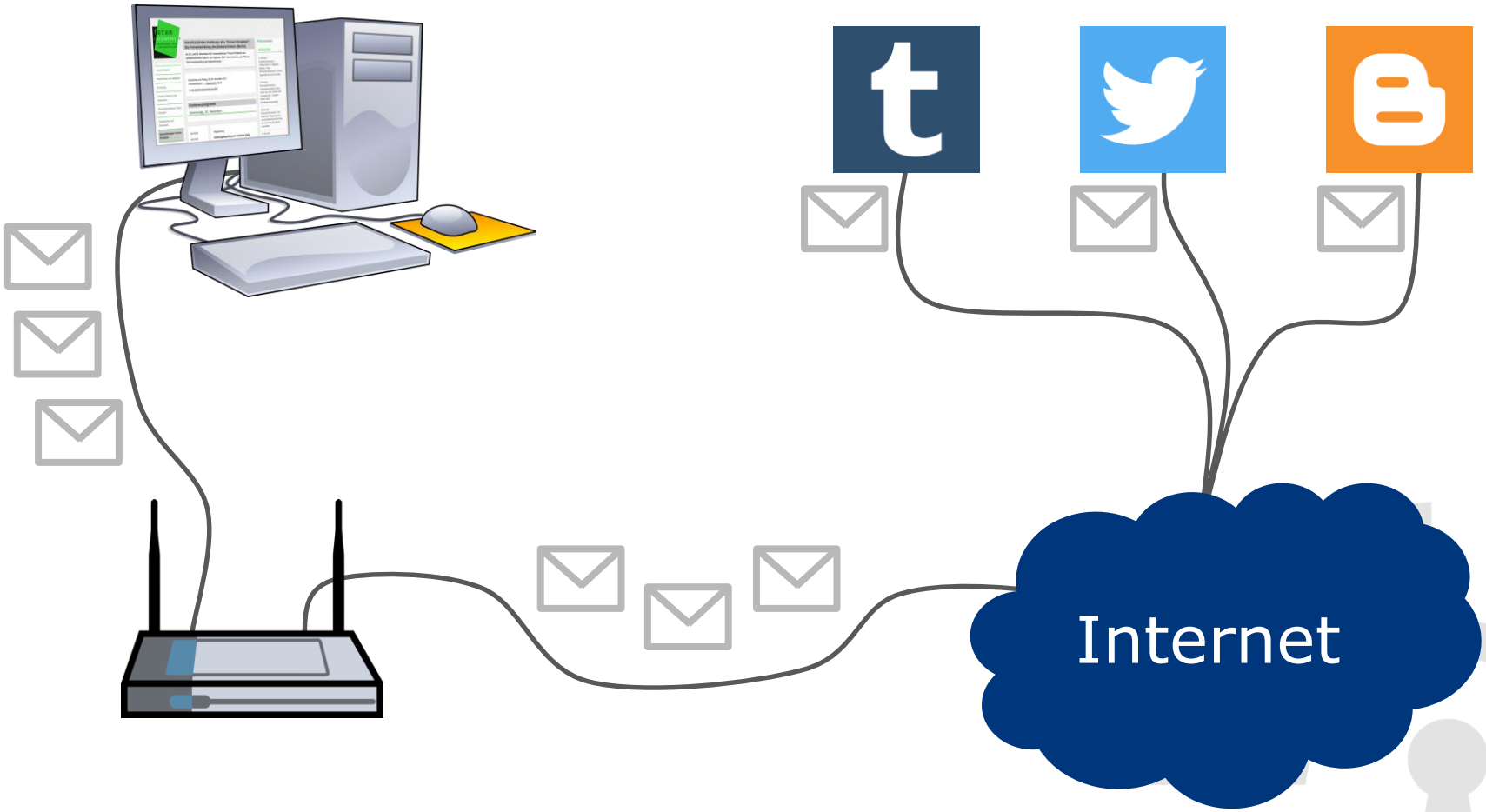
Lösungsvorschlag 2

Address Hopping

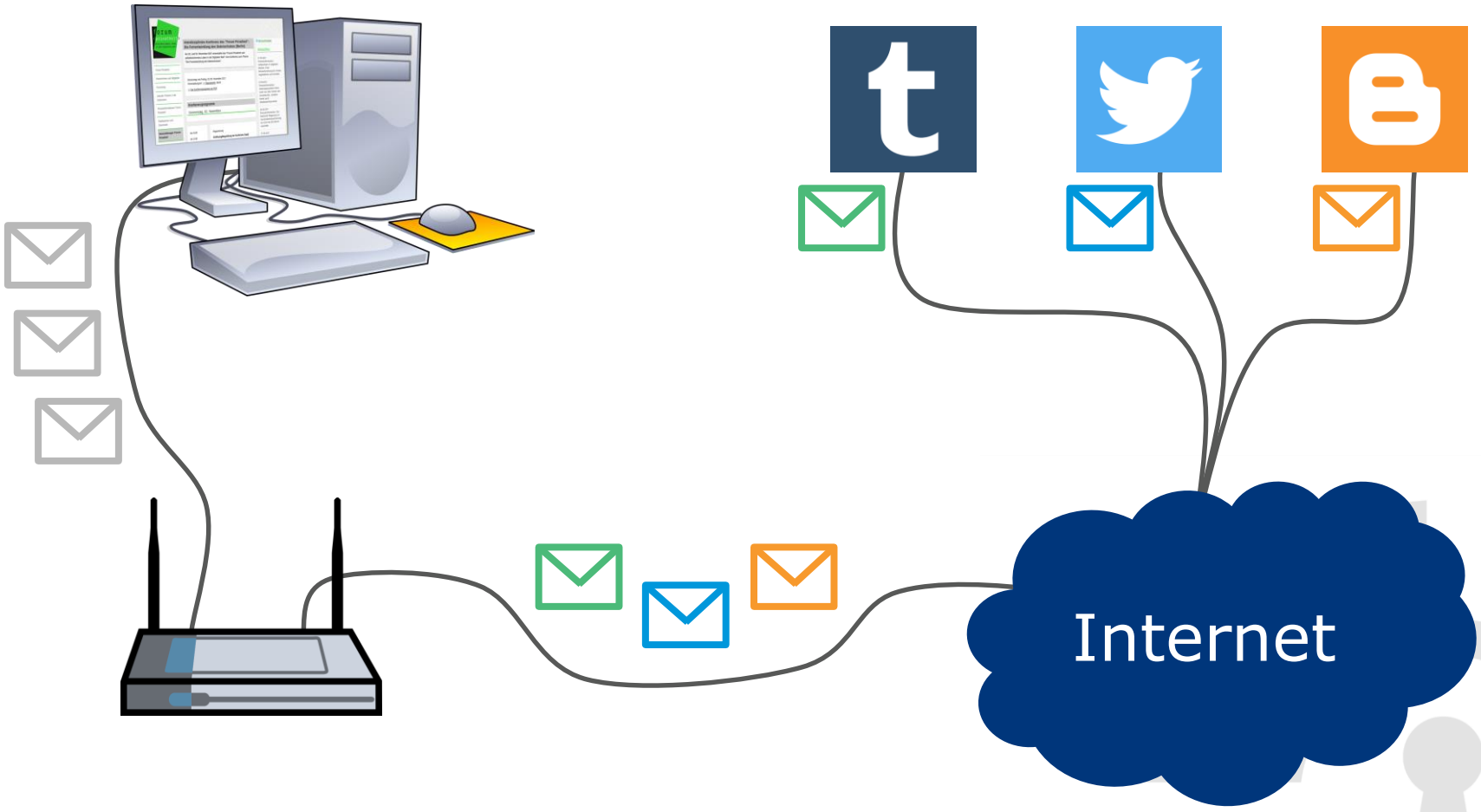
Häufiger Wechsel der IP-Adressen

- Nutzer verteilen ihren Traffic über mehrere Adressen gleichzeitig oder nutzen eine Adresse nur für einen kurzen Zeitraum
- Wegen der Größe des IPv6-Adressraumes möglich
- Nach IP-Adresswechsel können Tracker neue Nutzeraktivitäten nicht (ohne weiteres) mit alten verknüpfen

Adress Hopping - Architektur



Adress Hopping - Architektur



Address Hopping

Stand der Technik

- Jeder Nutzer hat zu jedem Zeitpunkt eine eindeutige IP-Adresse
- Nutzer erhalten täglich eine neue IP-Adresse
- IPv6 Privacy Extensions ändern regelmäßig (meist täglich) einen Teil der IPv6-Adresse

Anforderungen

- Bestehende Verbindungen sollen nicht unterbrochen werden
- IP-Adressen für ausgehende Verbindungen sollen häufig gewechselt werden
- Traffic im internen Netzwerk des Nutzers bleibt vom Adresswechsel unberührt

Address Hopping – Optionen

Naiver Ansatz

Eine neue IP-Adresse für jede neue Verbindung

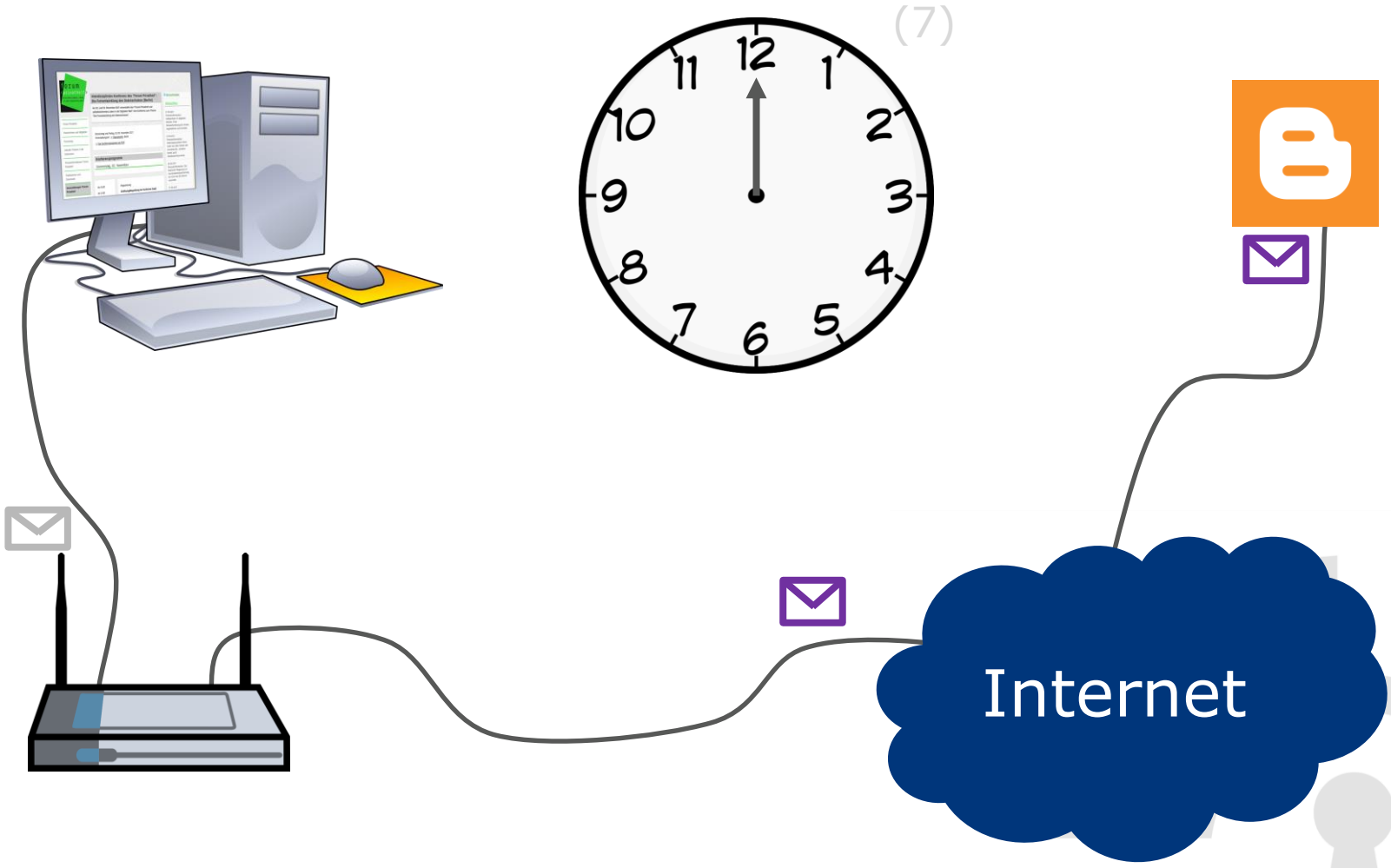
- Web-Anwendungen könnten Sitzungen terminieren, wenn sich die IP-Adresse während eines Besuches ändert

Verbesserung

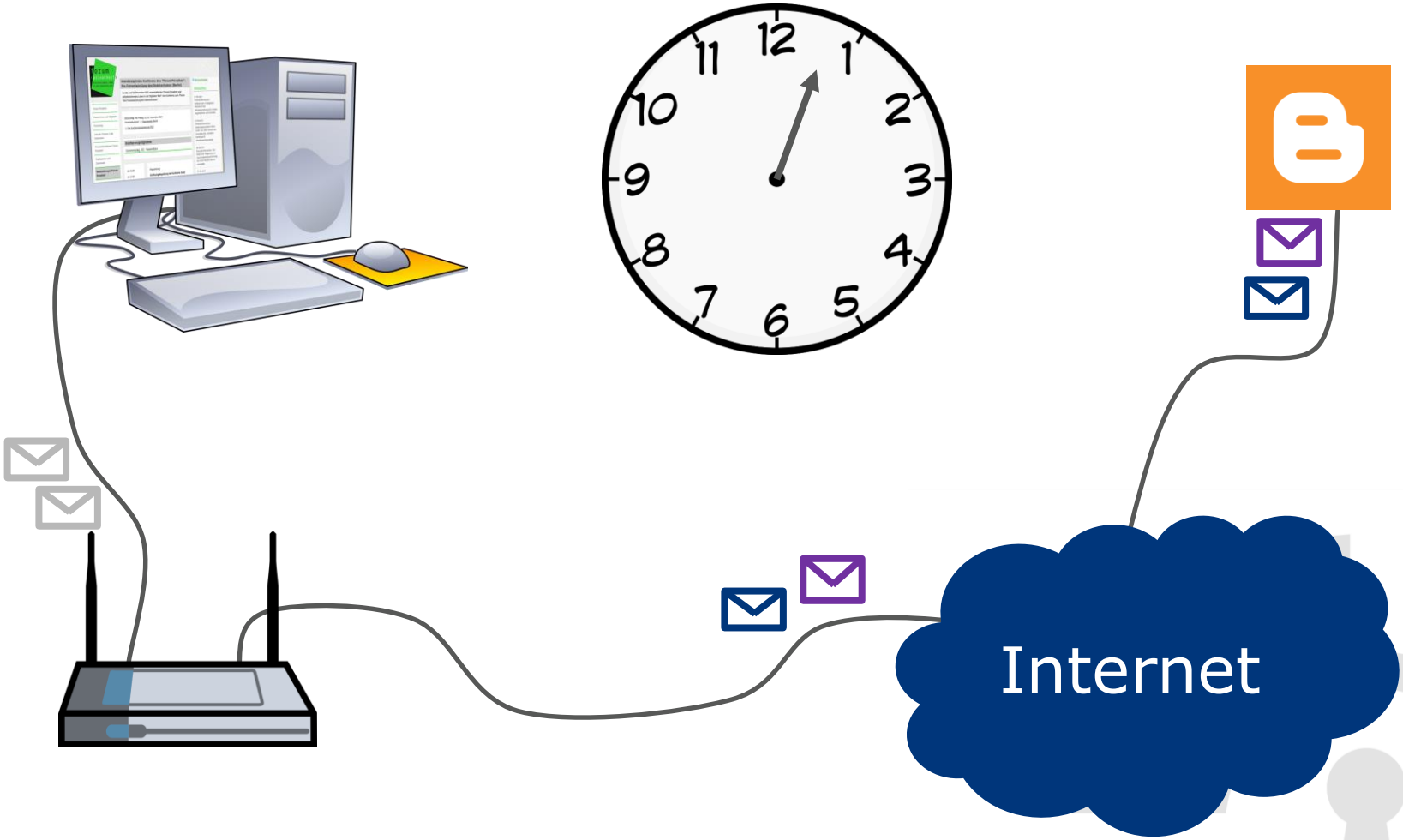
Wiederverwendung einer IP-Adresse für ein festes Ziel

- Höhere Komplexität
- Anfragen, die an ein festes Ziel gesendet werden, sind verknüpfbar

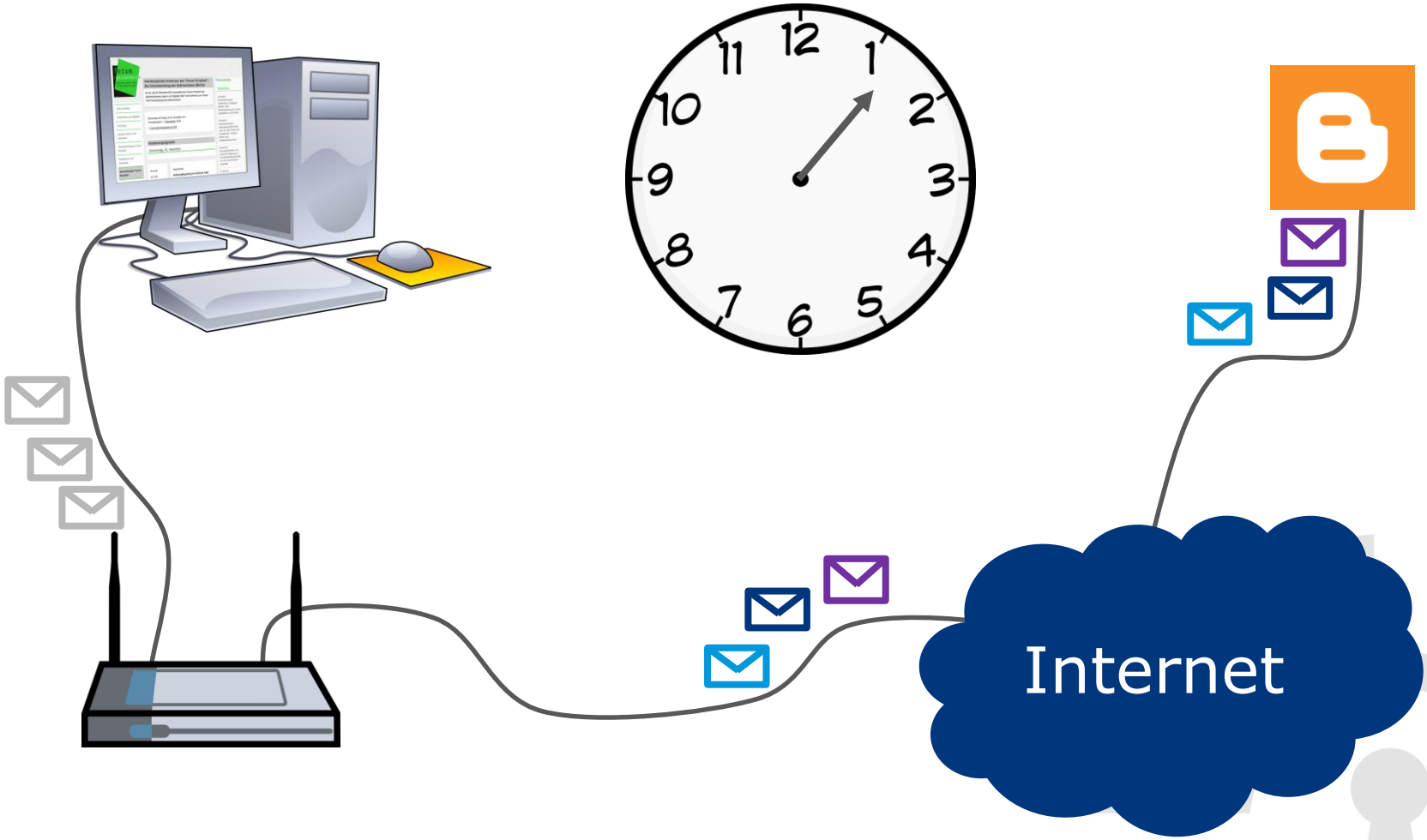
Address Hopping (zeitbasiert)



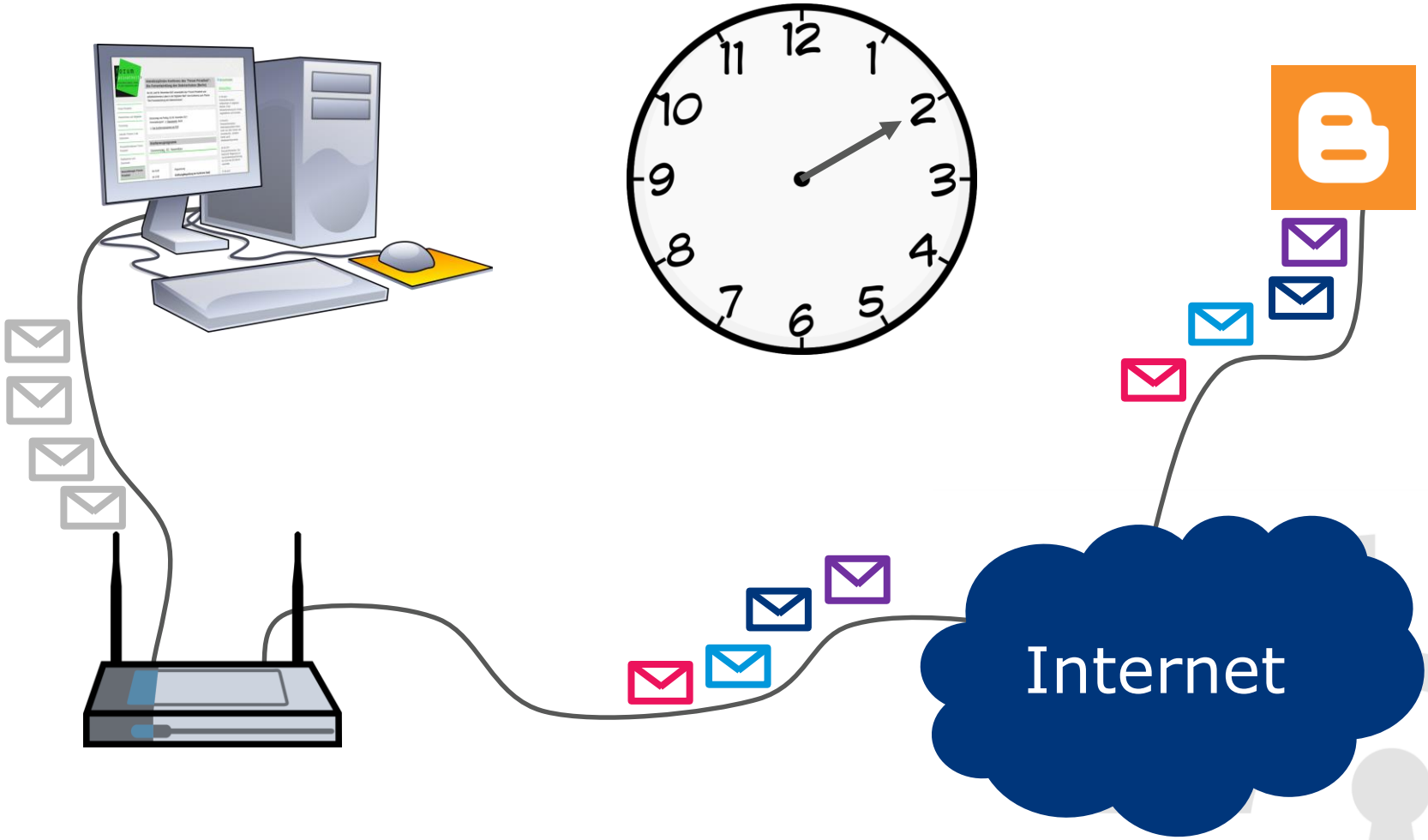
Address Hopping (zeitbasiert)



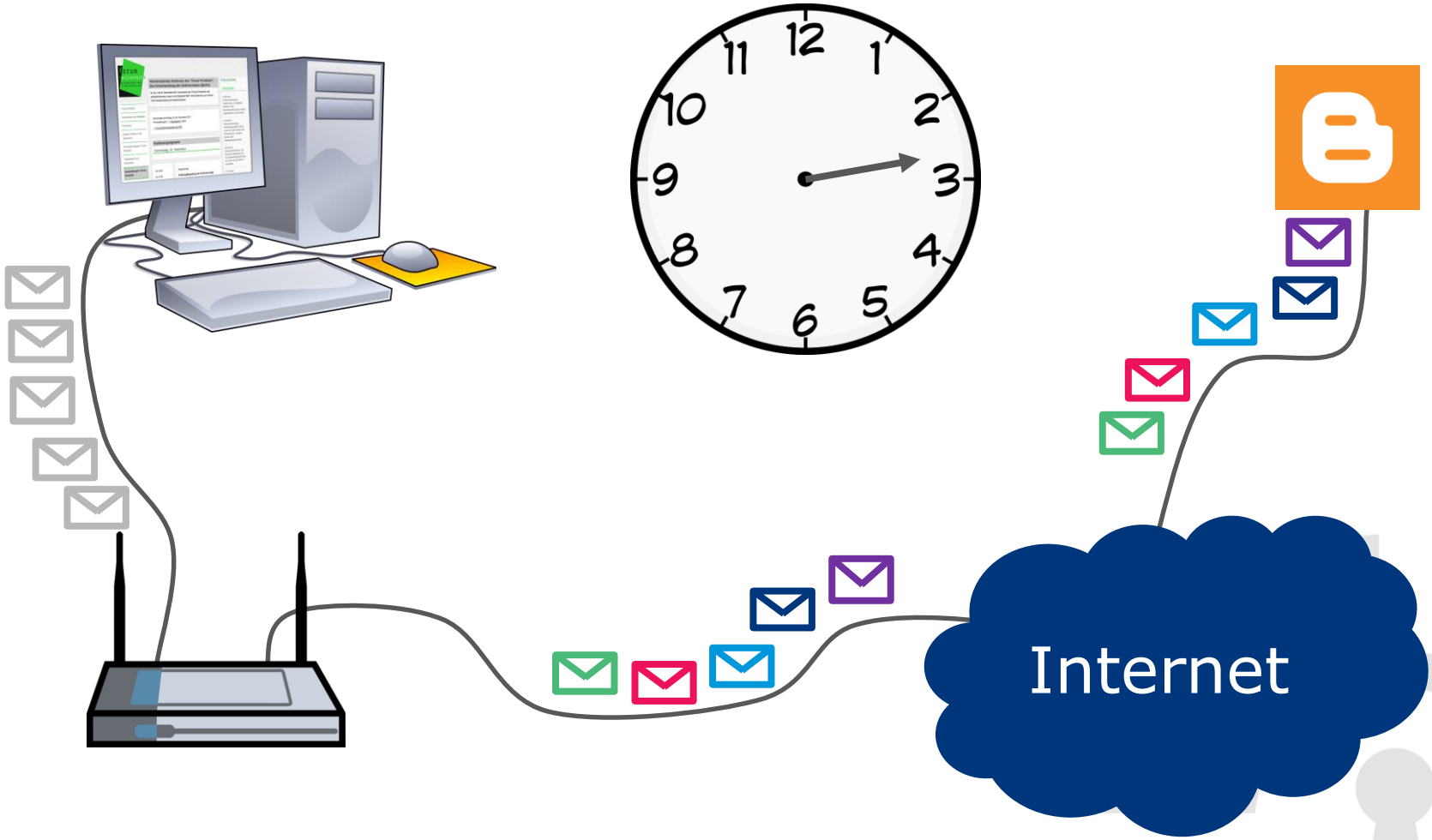
Address Hopping (zeitbasiert)



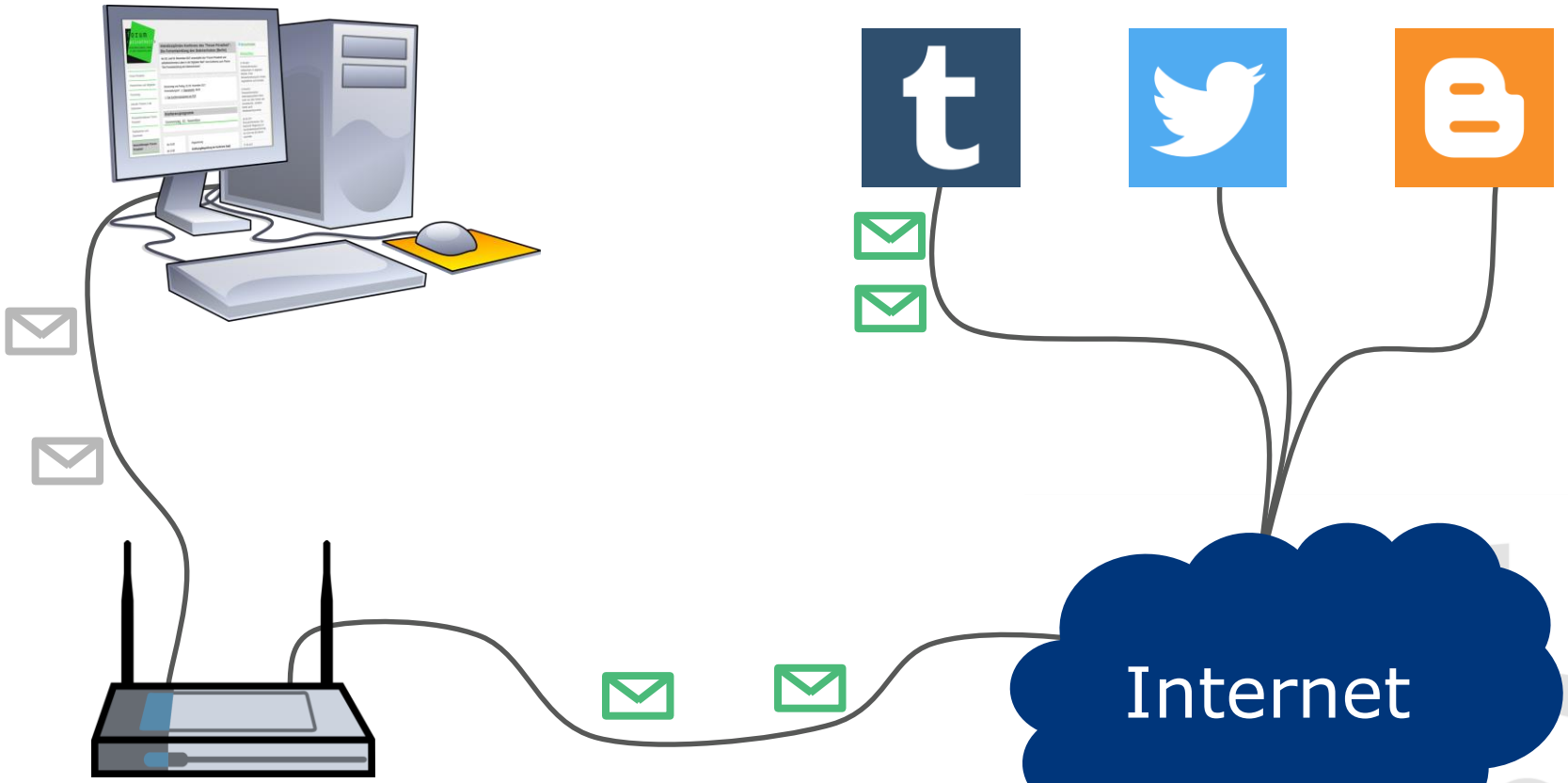
Address Hopping (zeitbasiert)



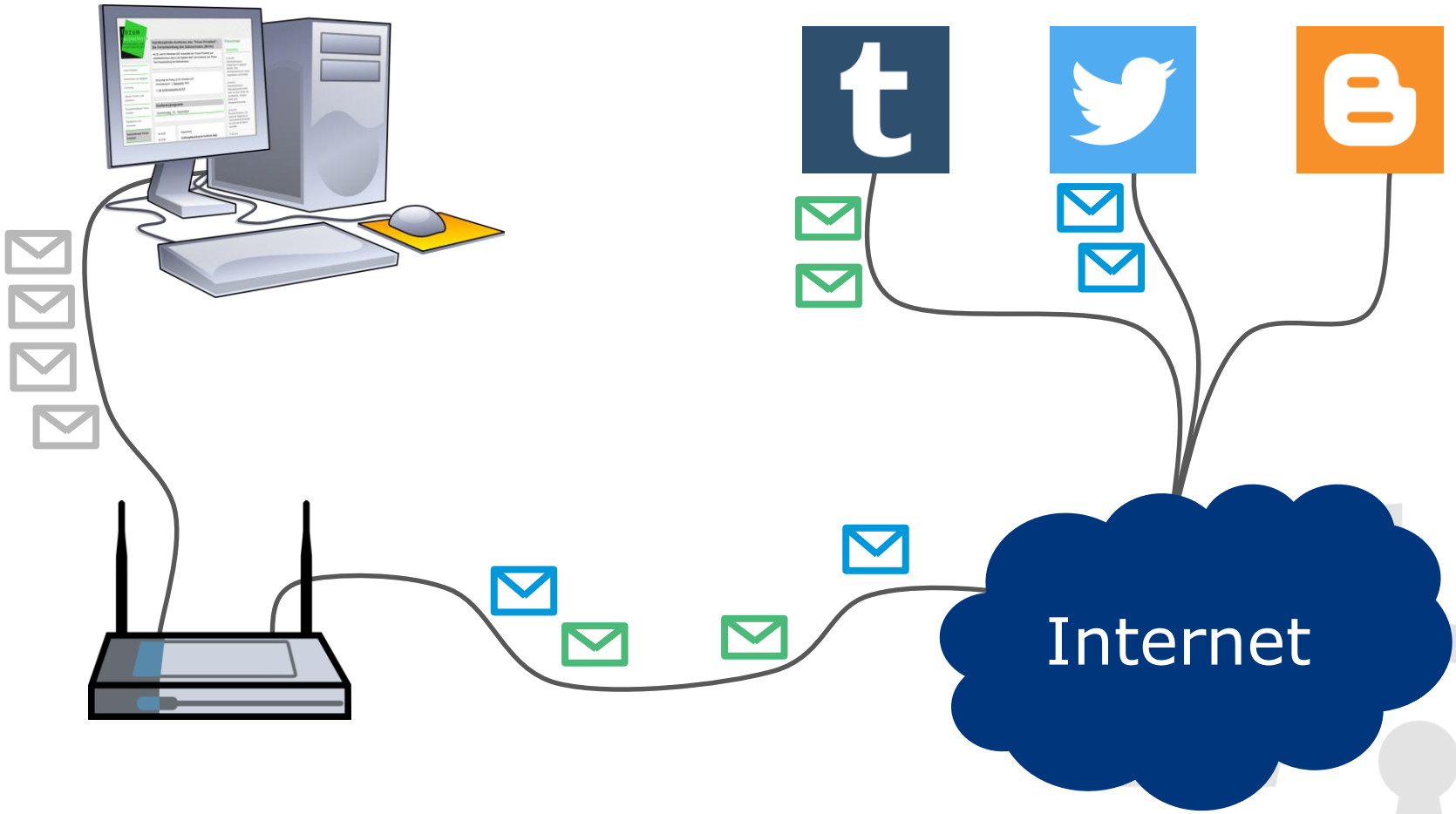
Address Hopping (zeitbasiert)



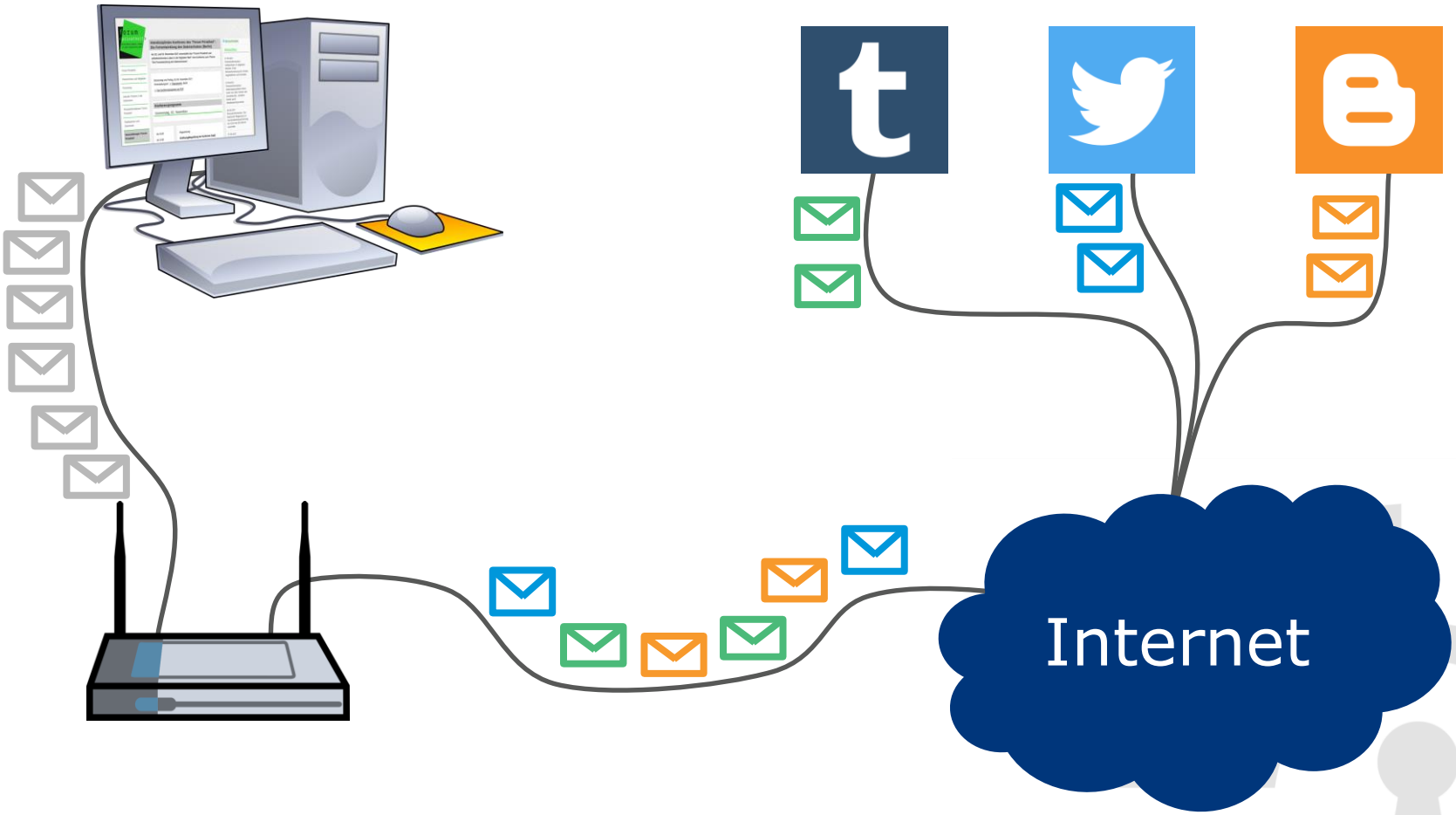
Address Hopping (zielbasiert)



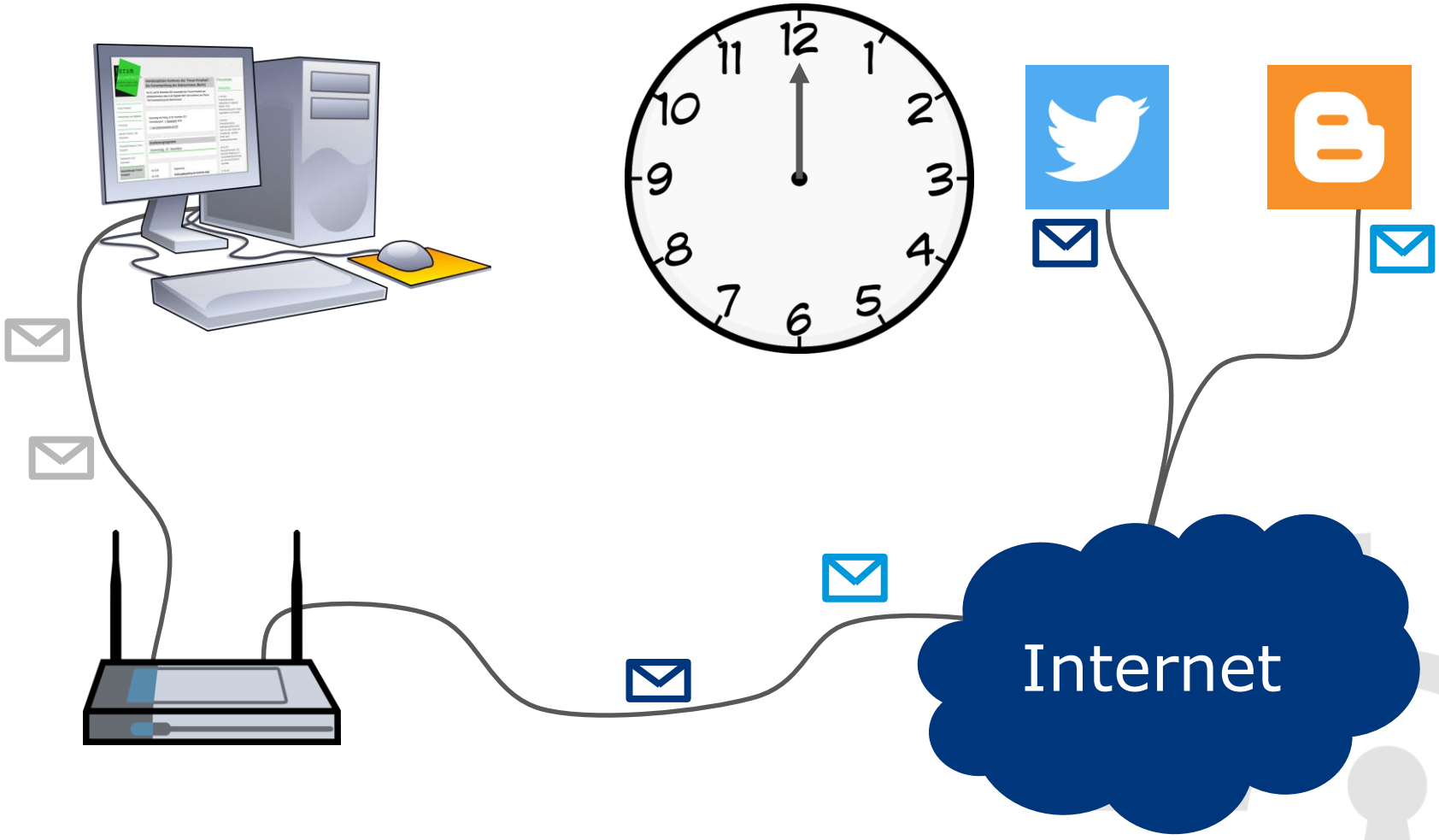
Address Hopping (zielbasiert)



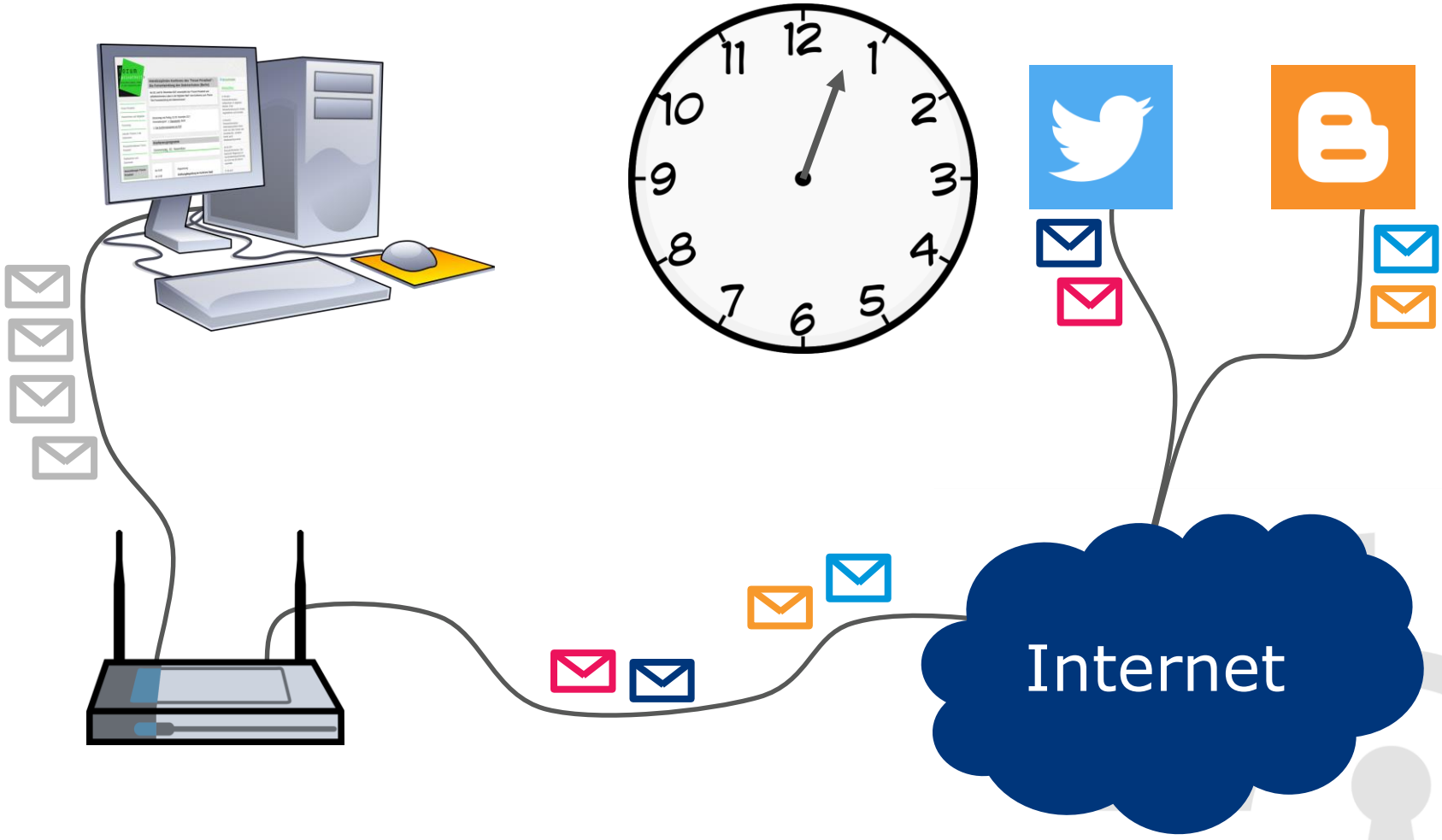
Address Hopping (zielbasiert)



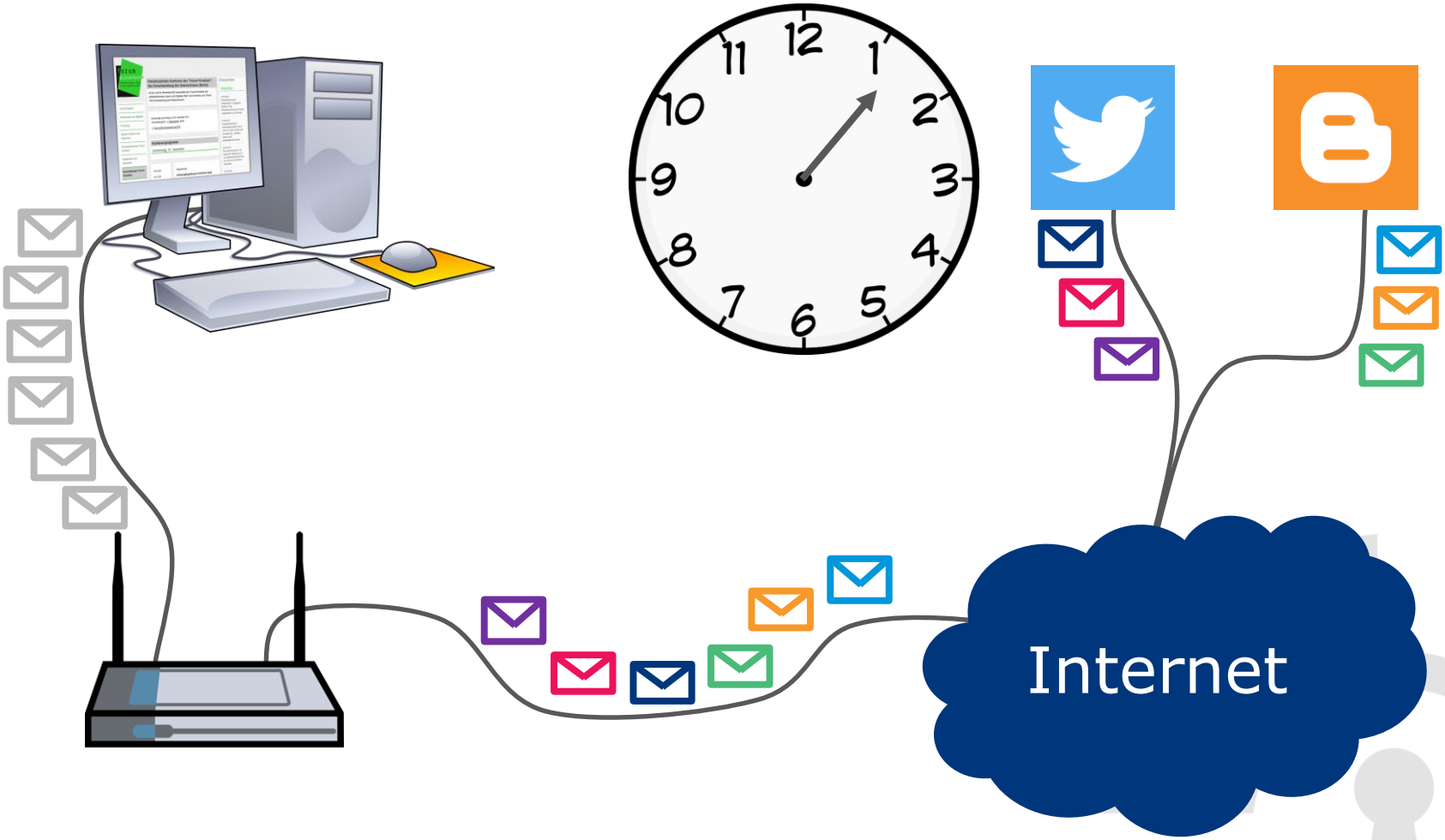
Address Hopping (kombiniert)



Address Hopping (kombiniert)



Address Hopping (kombiniert)



Proof of Concept

Umsetzung auf Raspberry 3

- WLAN-AP
- iptables und NFQUEUE
- conntrack
  - Connection Tracking für TCP, UDP, ICMP
  - Teil des Linux-Kernels

- Erfolgreiche Umsetzung für meistgenutzte Transportprotokolle TCP, UDP, ICMP

Evaluation

- Keine wahrnehmbare Zunahme der Latenz
  - Wenn es nicht zu viele neue Verbindungen pro Sekunde gibt
  - Beispiel: Spiegel Online

Werbung	Verbindungen	IP-Adressen	Dauer
Mit	103	47	9s
Ohne	43	12	4s

- (Bekannte) Probleme
  - Manche Webseiten terminieren Session bei IP-Adresswechsel
  - FTP funktioniert nicht
  - Flaschenhälse
    - Python → C
    - nfqueue → Daemon
    - iptables

Ausblick

- Behebung des Flaschenhalses durch Ersetzen von *iptables* durch *nftables*
- Ausführlichere Evaluation
- Feldtest in Zusammenarbeit mit einem ISP
  - 50 Router
- Schutz auf Netzwerk- **und** Anwendungsebene

Fazit

- Existierende Schutzmaßnahmen werden nicht breit genug eingesetzt
- Wir benötigen leichtgewichtige Anonymisierungslösungen
- **IP-Adresswechsel**
  Ein einfacher Basisschutz, der sich in die heutige Architektur des Internets integrieren lässt
  - Implementierung mittels iptables und NFQUEUE-Regeln

AN.ON
NEXT GENERATION

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Privatsphäre als inhärente Eigenschaft eines Kommunikationsnetzes

Matthias Marx – marx@informatik.uni-hamburg.de
Universität Hamburg – Sicherheit in verteilten Systemen

Literatur

- International Telecommunication Union. ICT Facts and Figures 2016. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf, 2016.
- The Tor Project. Tor metrics. https://metrics.torproject.org/userstats-relay-country.html, 2017.
- Dominik Herrmann, Christine Arndt, and Hannes Federrath. IPv6 prefix alteration: an opportunity to improve online privacy. arXiv preprint arXiv:1211.4704, 2012.
- Dominik Herrmann, Christian Banse, and Hannes Federrath. Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. Computers & Security 39 (2013): 17-33.
- Thomas Narten, Richard Draves, and Suresh Krishnan. Privacy extensions for stateless address autoconfiguration in IPv6 (RFC 4941), 2007.

Bildquellen

(1) Desktop-PC und Monitor, https://pixabay.com/en/computer-calculator-server-desktop-8563/, CC0 und Screenshot von https://www.forum-privatheit.de/

(2) WLAN-Router, https://openclipart.org/detail/129067/wireless-router, CC0

(3) Anand S, https://www.flickr.com/photos/root_node/3029241801, „Infy blog interests tag cloud", CC BY 2.0

(4) Sara 506, https://commons.wikimedia.org/wiki/File:Group_people_icon.jpg, „Group people icon", eingefärbt von Matthias Marx, CC BY-SA 3.0

(5) Schild, https://pixabay.com/en/shield-badge-logo-symbol-label-308943/, eingefärbt von Matthias Marx, CC0

(6) Soziale Netzwerke, https://www.flaticon.com/packs/social-networks-logos-2, designed by Freepik from Flaticon

(7) Ziffernblatt, https://openclipart.org/detail/28499/clock-face, CC0