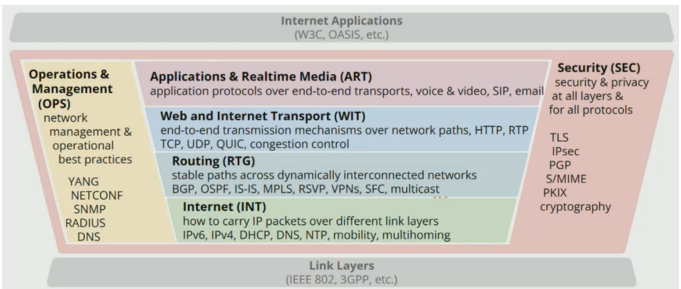
GUUG Sommerworkshop 2026

Das RIPE-Meeting 2026 in Edinburgh und die Konsequenzen für Unix

Erwin Hoffmann

[feh@fehcom.de]

25. Juli 2026



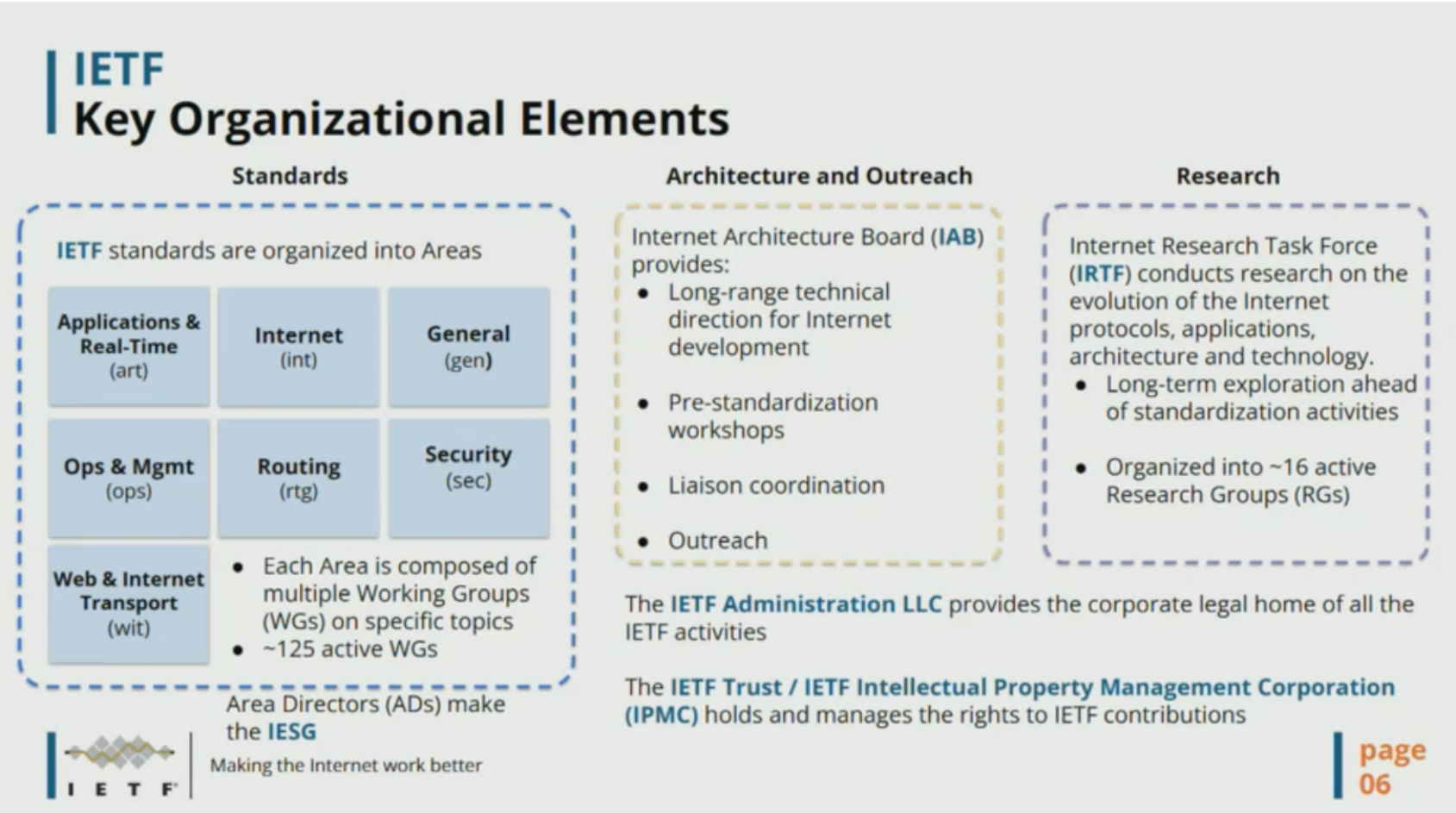
Überblick

Das RIPE 92 Meeting in Edinburg bot eine gute Gelegenheit zu eruieren, was sich unter dem Dach der IETF alles so tut. Das wollen wir hier kurz berichten, offene Punkte ansprechen, die nicht diskutiert wurden und speziell auch die Konsequenzen der Entwicklung für `*ix` Betriebssysteme betrachten.

- Dem Meeting voraus gab es 'Knatsch' zwischen der DNS-WG und dem IETF bezüglich des 'Retirements' der ENUM-Domain im DNS (Mapping von Telefon-Nummern auf IP-Adressen).
- Stunk gab es auch in der TLS Working Group bzgl. des Einsatzes von PQ bei TLS 1.3. Hier gab es geteilte Positionen zwischen den Befürwortern eine reinen - auf MLKEM - basierten Schlüsseltauschs und einer 'hybriden' Variante unter Einsatz von PQ und ECC.
- Im Kern ging es hierbei um die Art der Entscheidungsfindung: War das bisherige IETF-Verfahren darauf ausgelegt einen 'consensus' zwischen den WG-Mitgliedern (unter Moderation des *Area Directors*) zu erzielen, so wird nun teilweise von einem 'rough consensus' bzw. von Mehrheitsentscheidungen 'votes' gesprochen.
- Dies macht das Meeting so besonders, wobei hier auch die Kluft zischen den 'Ingenieuren' und den 'Operatoren' zu Überwinden versucht wurde.

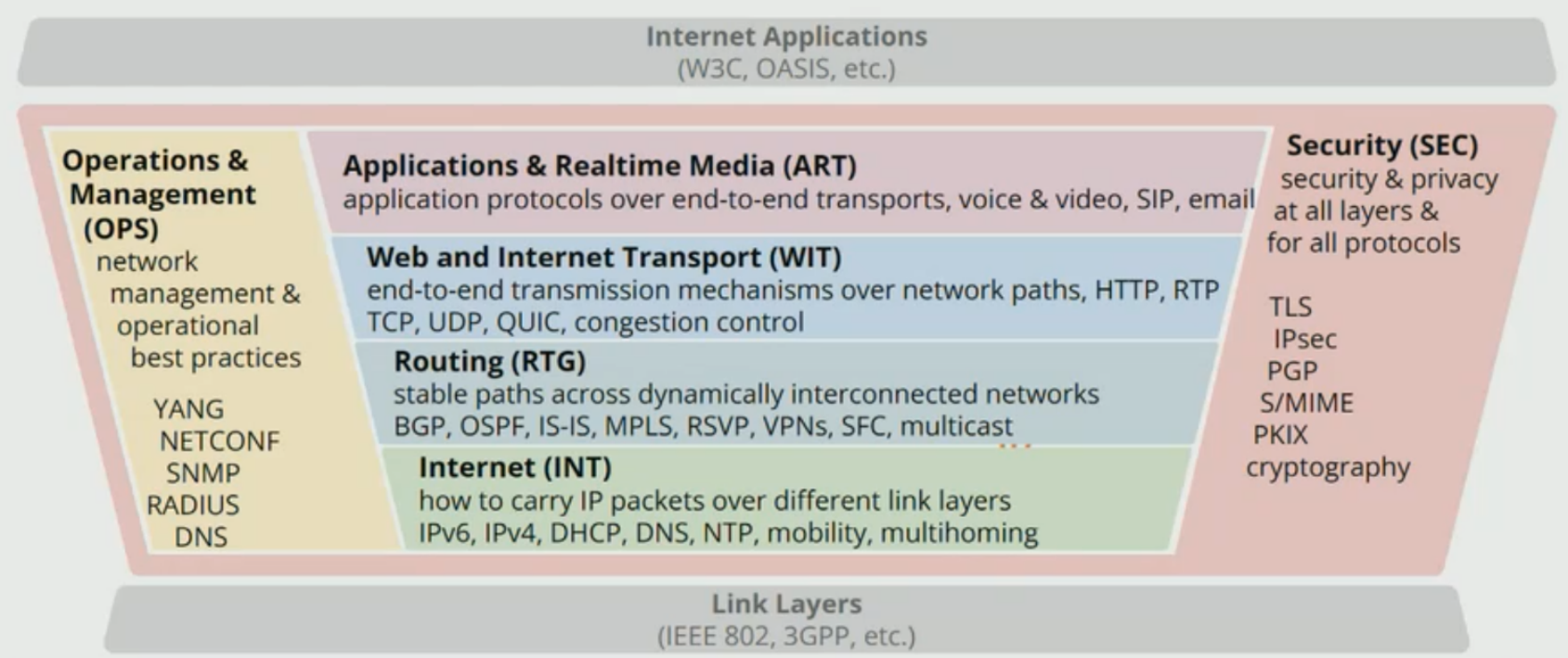
↪ Wir möchten hier keine Antworten oder Interpretationen geben, sondern den Blick auf kommende Szenarien erweitern, wo Netzwerke und der Einsatz von Unix erforderlich sind.

Die IETF Working Areas



↪ `https://www.ietf.org/technologies/areas/`

Die IETF Landkarte

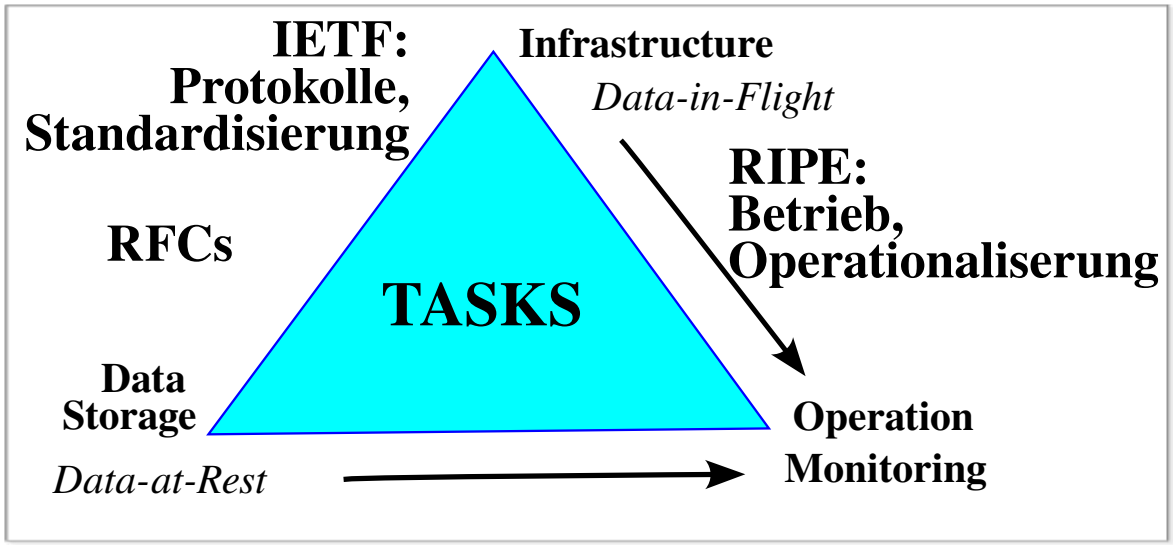


In Ergänzung zu diesen Areas, stehen noch die folgenden 'Technologien' im Fokus:

- Domain Name System: `https://www.ietf.org/technologies/dns/`
- Network Management: `https://www.ietf.org/technologies/netmgmt/`
- Internet of Things: `https://www.ietf.org/technologies/iot/`

↪ Viele Dinge scheinen mir mit 'heisser Nadel' gestrickt worden zu sein ...

Zusammenspiel von RIPE und IETF



↪ `https://www.rfc-editor.org/`

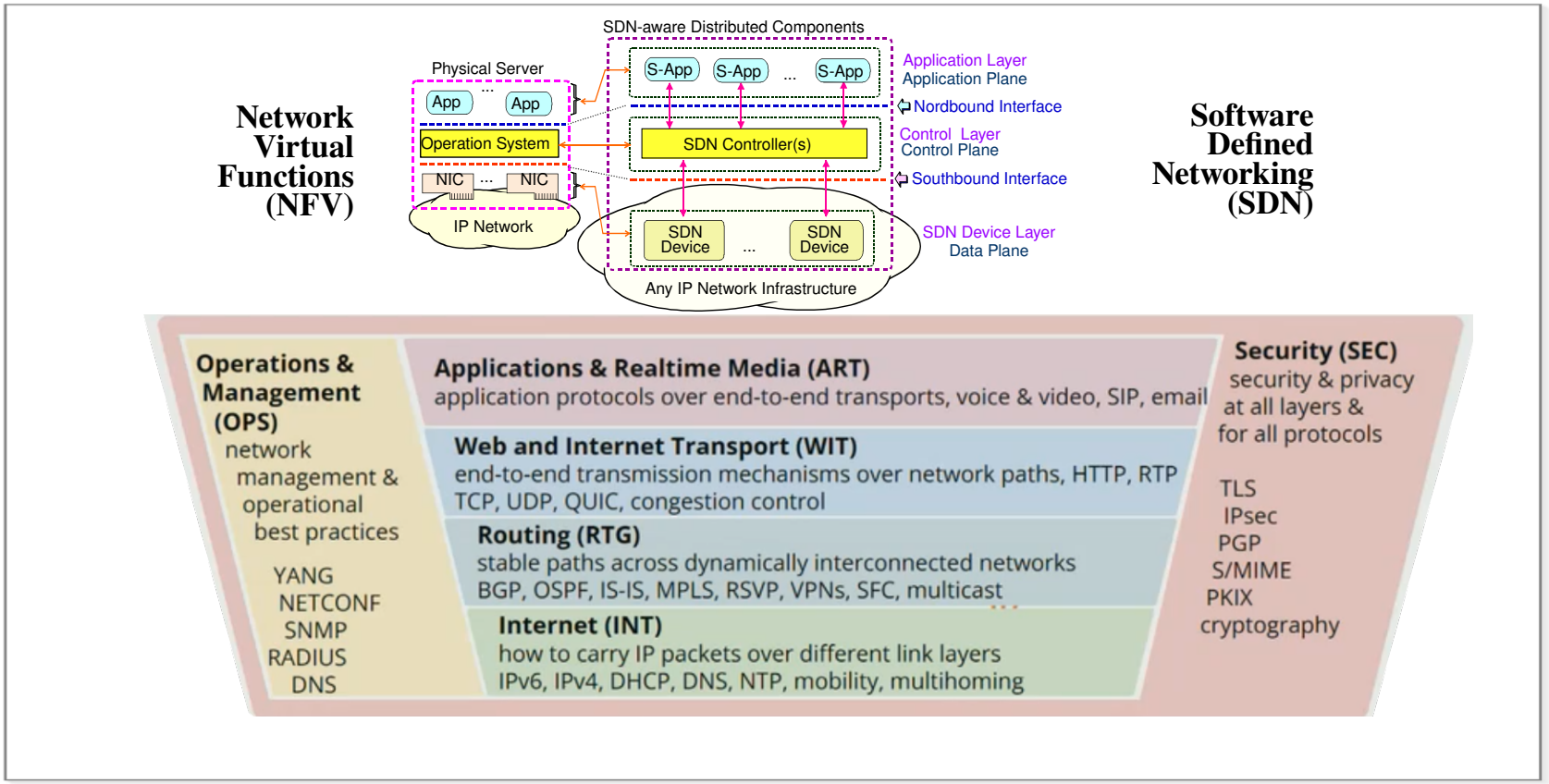
RFC 10014: »Guidelines for Characterizing the Term 'OAM'«

Kategorien:

- Internet/Proposed/Draft Standard
- Best Current Praxis
- Informational/Experimental
- Historic/Deprecated

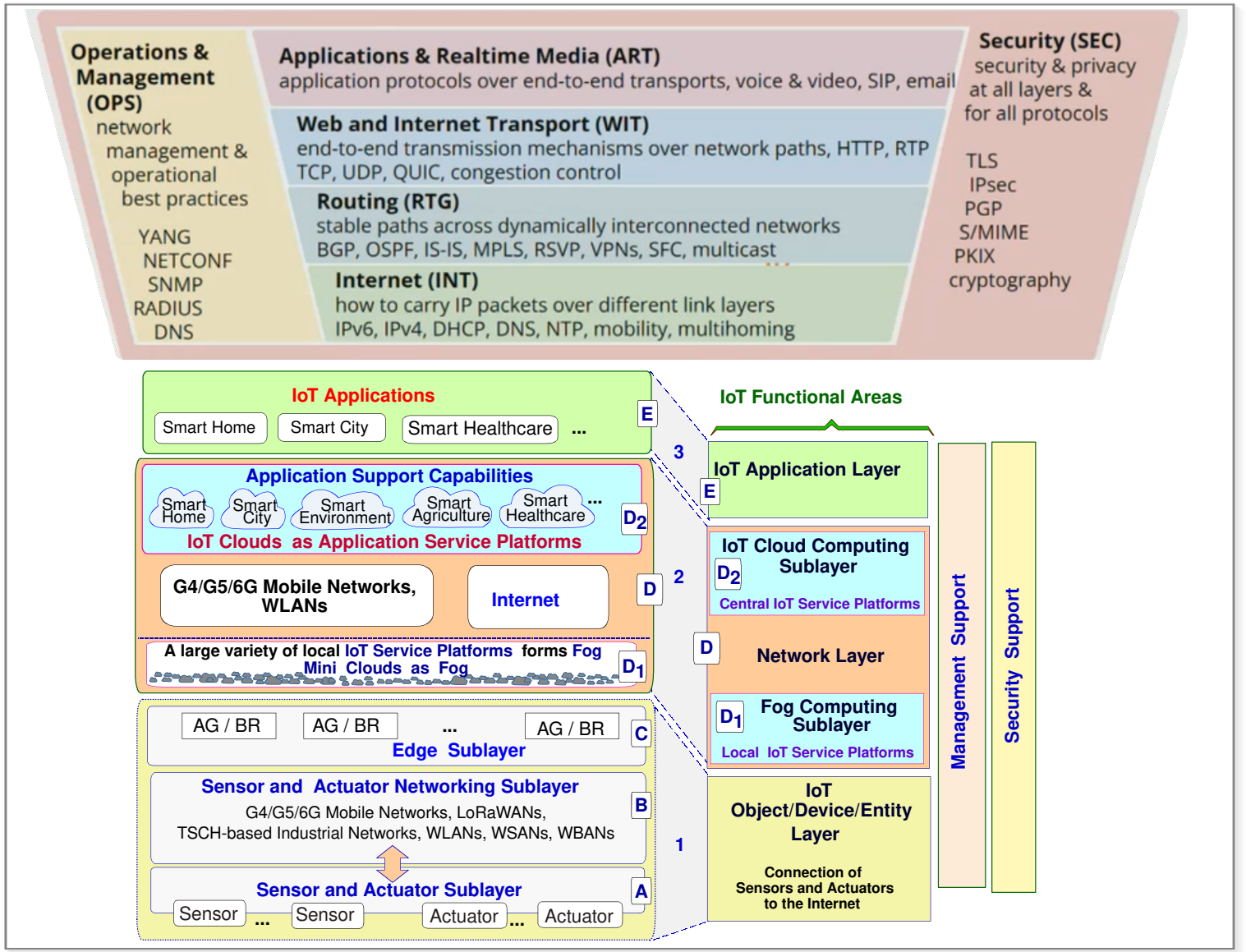
IETF stellt die Standardisierung im Bereich des Datentransports sicher, das RIPE übernimmt deren operative Umsetzung im Rahmen des Internet.

Die (SDN) Revolution findet (noch nicht) statt



↪ *Software Defined Networking* und *Network Function Virtualisation* sind wohl noch nicht ganz angekommen, obwohl die die Fortsetzung heutiger Virtualisierungs-Techniken sind.

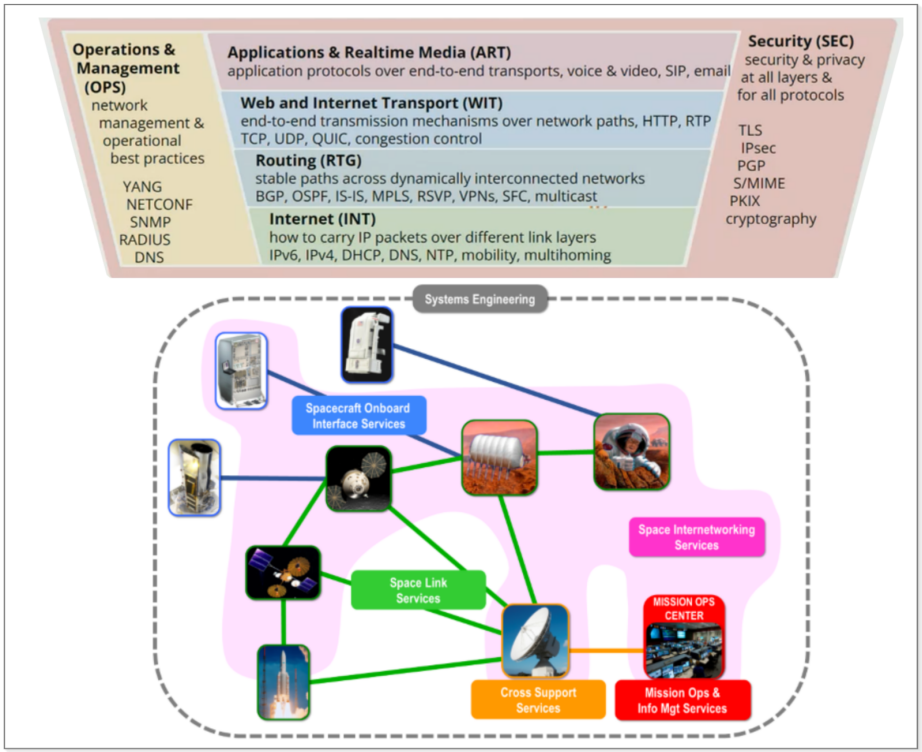
Auch das Internet of Things (IoT) ist noch nicht angekommen



Aber der 'Outer-Space' bekommt ein eigenes IPv6-Netz (RIR)

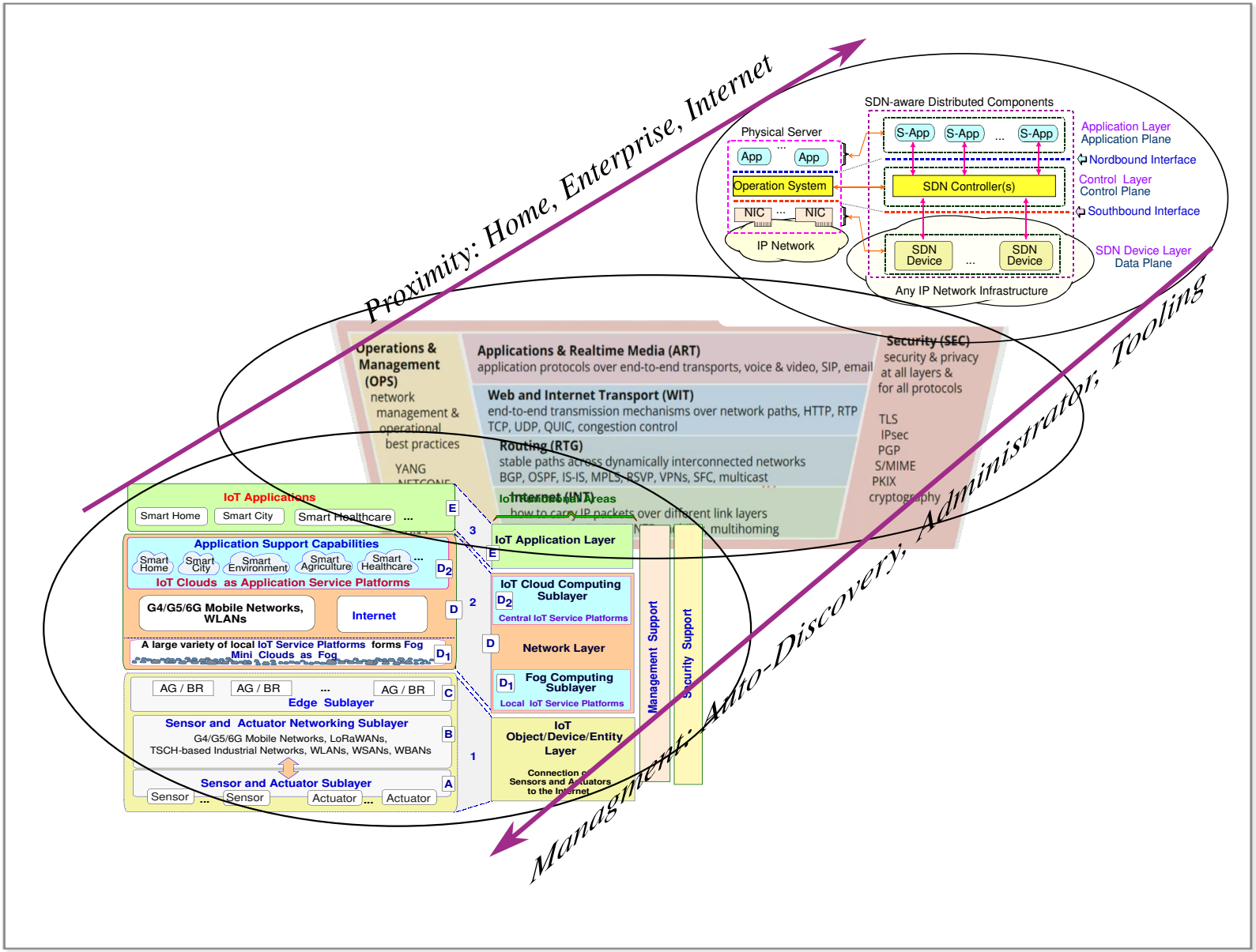
↪ `https://datatracker.ietf.org/doc/draft-li-tiptop-address-space/`:

> *»IP Address Space for Outer Space«*
> *The exploration of outer space depends heavily upon communications technology and in many cases, uses IP. IP address allocation has been formally assigned to Regional Internet Registries (RIRs), but there is no formal allocation of address space for networks in outer space.*



↪ Was sagt das '*Consultative Committee for Space Data Systems*' (`https://ccsds.org/publications/allpubs/`) dazu?

Provissioning, Administration, Management



Administration der Netze (Operation & Maintenance) OAM

Wie dargestellt, haben wir es mit dem Einsatz von Unix auf unterschiedlichen Ebenen 'Layers' zu tun:

- Der IoT-Bereich:
  - Der Einsatz hier ist von 'Autoconfiguration' geprägt.
  - IPv6 Multicast-Dienste sind hier gefordert.
- Der Access- oder Workstation-Bereich:
  - Verzicht auf LANs; Rechner werden an (Layer 3) Access-Switche angeschlossen (wie bei WiFi).
  - Connectivität über IPv6-only oder mittels VxLANs?
  - IPv4 Connectivity über CLAT; keine Broadcasts mehr (ARP); RFC 7335.
- Der Enterprise-Bereich:
  - Neue Routing Protokolle (SRv6, RFC 9855).
  - Administration der Endgeräte (YANG, NETCONF, RESTCONF): `https://wiki.ietf.org/group/ops/yang-security-guidelines`
- Der Provider-Bereich:
  - Daten-Transport: Multi-Pathing QUIC?
  - Interdomain Routing mit BGP-4.
  - Sicheres Interdomain-Routing (Authentication/Authorization) mittels *Route Origin Autorizations* (ROA) beheimatet bei den Regional Internet Registries (RIR) auf Grundlage der *Resource Public Key Infrastructure* (RPKI).

↪ RIPE und IETF setzen auf IPv6; IPv4 ist Vergangenheit und wird nur noch geduldet.

Replik: Das B-ISDN Referenzmodell

Die ETSI (*European Telecommunications Standards Institute*) hat bereits 1995(!) das sog. B-ISDN Referenzmodell eingeführt:

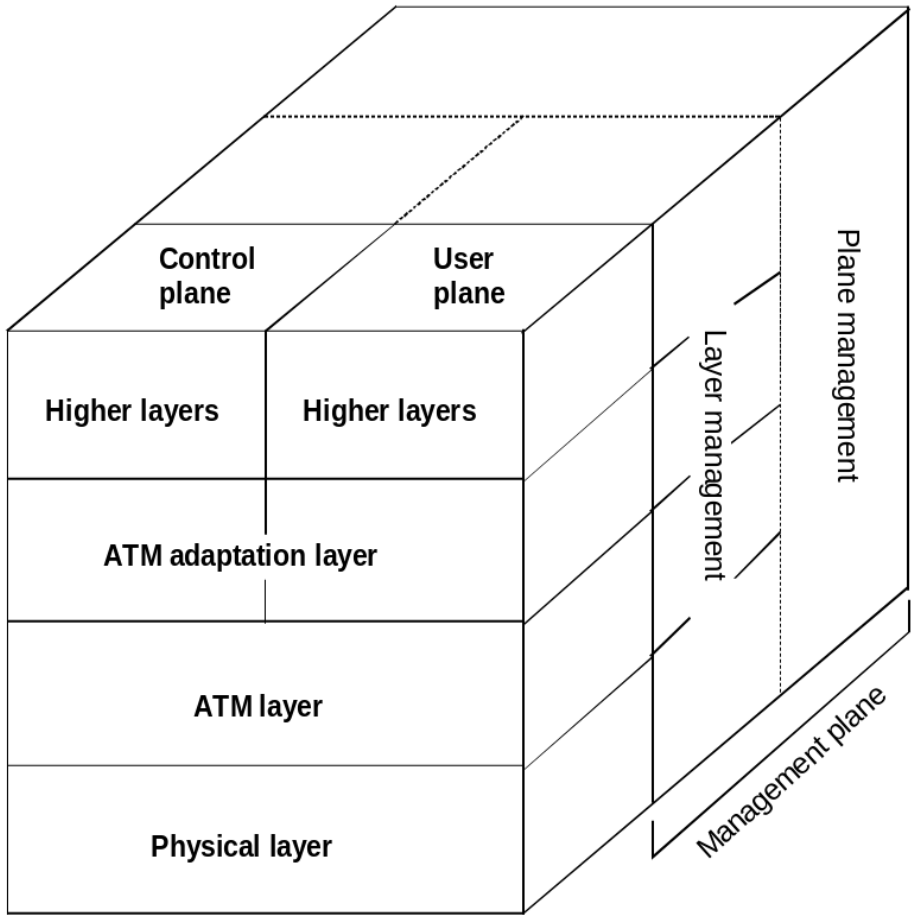


Figure 1: B-ISDN PRM

- User Plane → Daten
- Control Plane → IS-IS Routing, SS7

Unix und der Datentransport

- Für den «Datentransport» werden beim RIPE nur noch die Protokolle HTTP und RTP (*Real-Time Transport Protocol*) (vor)gesehen.
- QUIC (für Web), UDP (für DNS und RTP) sowie TCP (für alles andere) stellen den eigentlichen Transport bereit.

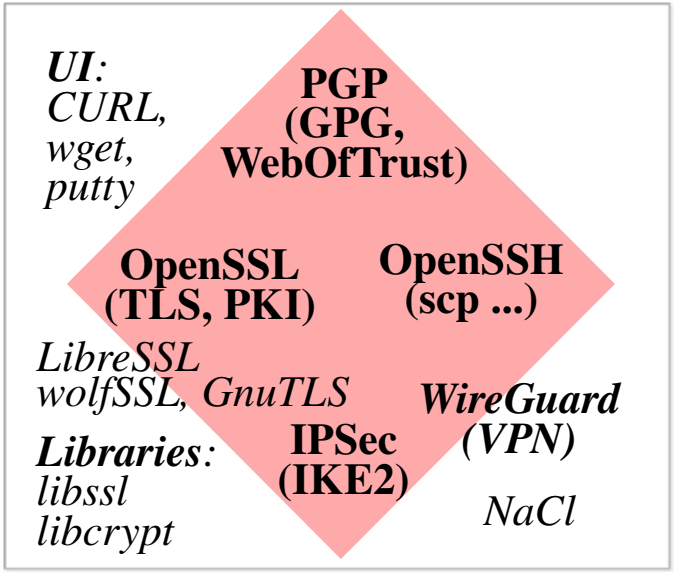
↪ QUIC verlangt TLS-Verschlüsselung. Um die performant zu machen, müssen sie vom User-Space in den Kernel-Space verlagert werden. Dies ist Gegenstand der aktuellen OpenSSL Versionen.

↪ Um unterschiedliche Datenpfade und -carrier zu unterstützen, wird entweder MultiPathing (TCP) oder gerichtete Verbindungen (wie bei MPLS) benötigt. QUIC liefert das noch nicht: Für das (UDP-) Paketmanagement sind die einzelnen Knoten unabhängig voneinander zuständig und dies gestaltet sich zudem aufwändig. Ob QUIC für alle Transportszenarien eine günstige Wahl darstellt, bleibt abzuwarten.

↪ Wie es mit TLS (1.3) weitergeht, ist unklar: Vom IETF (der WG) wird alleiniges ML-KEM als Schlüsselaustausch-Protokoll favorisiert, eine qualifizierte Minderheit sieht eine Kombination von ML-KEM und ECC als hybrides Verfahren vor.

Unix und Privacy

Die Unix-Welt hat vier kryptographischen Fundamente:



- OpenSSH wird massgeblich von den OpenBSD-Leuten entwickelt.
- OpenSSL (TLS, PKI) und IPSec unter Federführung der IETF mit starkem Einfluss der NSA.

↪ Die Crypto-Algorithmen (und ihre Umsetzung) haben massgeblichen Einfluss auf unsere Internet *Privacy*. In den IETF-Gremien 'sitzen' im wesentlichen Leute grosser Firmen (Hyperscalern) und öffentlicher Institutionen, wie der NSA, unter Einbeziehung der Standardisierungen aus der NIST (*National Institute of Standards and Technology*) und der FIPS (*Federal Information Processing Standard*, z.B. FIPS-203 `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf`).

IPv6-mostly im Jahr 2026

Themen

- Die IP Versionen
- v4
  - NAT
  - NAT traversal
  - SNI
- v6
  - NAT64/DNS64
  - hacked64
  - 464XLAT
  - Implementierung
  - ipv6-mostly@home
  - Du hast noch kein IPv6?

Jannis M. Hoffmann
25. Juli 2026*

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).
- Folge: Die Anzahl an verwendeten IPv4 Adressen muss gesenkt werden.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).
- Folge: Die Anzahl an verwendeten IPv4 Adressen muss gesenkt werden.
- CIDR hat die Situation etwas entschärft.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).
- Folge: Die Anzahl an verwendeten IPv4 Adressen muss gesenkt werden.
- CIDR hat die Situation etwas entschärft.
- IPv6 hat $2^{45} \approx 3{,}5 \cdot 10^{13}$ /48 GUA Präfixe (sites) und ist noch erweiterbar.

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).
- Folge: Die Anzahl an verwendeten IPv4 Adressen muss gesenkt werden.
- CIDR hat die Situation etwas entschärft.
- IPv6 hat $2^{45} \approx 3{,}5 \cdot 10^{13}$ /48 GUA Präfixe (sites) und ist noch erweiterbar.
- IPv6 macht einiges besser (größere MTU, Mobile IP, Segment Routing, einfacheres Failover, SLAAC, flow labels)

Die IP Versionen

- Es gibt etwa 3,7 Milliarden global nutzbare Unicastadressen.
- Im Januar 2011 hat die IANA den letzten Block vergeben.
- Bei den RIRs sind unter ein Prozent der Adressen im freien Umlauf.
- IPv4 Adressen kosten bei Hostern inzwischen Geld (z.Z. $ 3-4 pro Monat).
- Folge: Die Anzahl an verwendeten IPv4 Adressen muss gesenkt werden.
- CIDR hat die Situation etwas entschärft.
- IPv6 hat $2^{45} \approx 3{,}5 \cdot 10^{13}$ /48 GUA Präfixe (sites) und ist noch erweiterbar.
- IPv6 macht einiges besser (größere MTU, Mobile IP, Segment Routing, einfacheres Failover, SLAAC, flow labels)
- Manches ist aber auch komplex: Path MTU Discovery macht Verbindungen auf Layer 3 zustandsbehaftet

NAT

- source NAT für Clients $\rightarrow$ mehre Clients teilen sich eine IP
- Probleme mit und durch
  - Zustandbehaftetem Routing
  - Client-to-Client und Server-to-Client Kommunikation
  - Videokonferenzen und VoIP
  - IP Blockierungen treffen viele

NAT

- source NAT für Clients $\rightarrow$ mehre Clients teilen sich eine IP
- Probleme mit und durch
  - Zustandbehaftetem Routing
  - Client-to-Client und Server-to-Client Kommunikation
  - Videokonferenzen und VoIP
  - IP Blockierungen treffen viele
- Wahrscheinlich schon milliardenfach im Einsatz

NAT

- source NAT für Clients $\rightarrow$ mehre Clients teilen sich eine IP
- Probleme mit und durch
  - Zustandbehaftetem Routing
  - Client-to-Client und Server-to-Client Kommunikation
  - Videokonferenzen und VoIP
  - IP Blockierungen treffen viele
- Wahrscheinlich schon milliardenfach im Einsatz
- CGNAT (doppeltes NAT) 100.64.0.0/10, häufig auch 10.0.0.0/8
- wird viel im Mobilfunk verwendet, z.T. auch für Privatkunden

NAT traversal

- destination NAT (statisch)
- UPnP
- STUN (UDP-only*)
- TURN (Relay)

NAT traversal

- destination NAT (statisch)
- UPnP
- STUN (UDP-only*)
- TURN (Relay)
- UDP-for-the-win (QUIC)

NAT traversal

- destination NAT (statisch)
- UPnP
- STUN (UDP-only*)
- TURN (Relay)
- UDP-for-the-win (QUIC)
- STUN ist auch nützlich für IPv6 Clients hinter einer Firewall

SNI

- Server Name Indication (SNI) für Server (HTTP/1.1 oder TLS)
- Spart IP Adressen für Server
- kennt man vom klassischem Webhosting

SNI

- Server Name Indication (SNI) für Server (HTTP/1.1 oder TLS)
- Spart IP Adressen für Server
- kennt man vom klassischem Webhosting
- reverse Proxy Layer 4 (HA-Proxy) oder Layer 7

SNI

- Server Name Indication (SNI) für Server (HTTP/1.1 oder TLS)
- Spart IP Adressen für Server
- kennt man vom klassischem Webhosting
- reverse Proxy Layer 4 (HA-Proxy) oder Layer 7
- Es können auch die neuen DNS RRs HTTPS und SVCB für Multiplexing genutzt werden,
- z.B. in Kombination mit einem destination NAT.

SNI

- Server Name Indication (SNI) für Server (HTTP/1.1 oder TLS)
- Spart IP Adressen für Server
- kennt man vom klassischem Webhosting
- reverse Proxy Layer 4 (HA-Proxy) oder Layer 7
- Es können auch die neuen DNS RRs HTTPS und SVCB für Multiplexing genutzt werden,
- z.B. in Kombination mit einem destination NAT.
- Ist mit IPv6 überflüssig?
- Loadbalancing von Webseiten im RZ mit EVPN?

NAT64/DNS64

- IPv6 only $\rightarrow$ bricht direkte Nutzung von v4-Adressen.

NAT64/DNS64

- IPv6 only $\rightarrow$ bricht direkte Nutzung von v4-Adressen.
- Nutzt `64:ff9b::/96` als Präfix
- IPv4 Adresse wird in die letzten 32 Bit codiert

NAT64/DNS64

- IPv6 only $\rightarrow$ bricht direkte Nutzung von v4-Adressen.
- Nutzt `64:ff9b::/96` als Präfix
- IPv4 Adresse wird in die letzten 32 Bit codiert
- Synthetische DNS Records wenn kein AAAA aber A Record vorhanden ist

NAT64/DNS64

- IPv6 only $\rightarrow$ bricht direkte Nutzung von v4-Adressen.
- Nutzt `64:ff9b::/96` als Präfix
- IPv4 Adresse wird in die letzten 32 Bit codiert
- Synthetische DNS Records wenn kein AAAA aber A Record vorhanden ist
- mit PREF64 oder RA für den Präfix wenn separater Router verwendet wird
- PLAT/NAT64 ist wie klassisches source NATv4 + SIIT

hacked64

- verwendet NAT64
- Patchen der libc um Funktionsaufrufe umzuschreiben
- klappt nur wenn libc verwendet wird
- TNAT64 [3]

hacked64

- verwendet NAT64
- Patchen der libc um Funktionsaufrufe umzuschreiben
- klappt nur wenn libc verwendet wird
- TNAT64 [3]
- Syscall überschreiben um in v6 umzuschreiben

464XLAT

- verwendet NAT64
- Client stellt CLAT bereit
- Besitzt synthetische IPv4 Adresse (aus 192.0.0.0/29)
- CLAT schreibt IPv4-Adressen beim Senden/Empfang um

464XLAT

- verwendet NAT64
- Client stellt CLAT bereit
- Besitzt synthetische IPv4 Adresse (aus 192.0.0.0/29)
- CLAT schreibt IPv4-Adressen beim Senden/Empfang um
- Pakete leicht größer (MTU+20 Byte) zum PLAT

Implementierung

- SIIT

Implementierung

- SIIT
- CLAT (client), PLAT (server)

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)
- RA für PREF64 (client & server)

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)
- RA für PREF64 (client & server)
- DNS64 im Client (optional)

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)
- RA für PREF64 (client & server)
- DNS64 im Client (optional)
- **Saubere Integration in Netzwerkclients.**

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)
- RA für PREF64 (client & server)
- DNS64 im Client (optional)
- **Saubere Integration in Netzwerkclients.**
- Wird unterstützt in iOS, OS X und Android
- Kommt in Windows 11 (preview) und NetworkManager (Linux) nächster Monat?

Implementierung

- SIIT
- CLAT (client), PLAT (server)
- DHCPv4 Option 108 (client & server)
- RA für PREF64 (client & server)
- DNS64 im Client (optional)
- **Saubere Integration in Netzwerkclients.**
- Wird unterstützt in iOS, OS X und Android
- Kommt in Windows 11 (preview) und NetworkManager (Linux) nächster Monat?
- 464XLAT Wird schon von Mobile ISPs eingesetzt.

ipv6-mostly@home

- Raspberry Pi

ipv6-mostly@home

- Raspberry Pi
- im eigenen Layer 2 Netz (VLAN) ohne DHCP

ipv6-mostly@home

- Raspberry Pi
- im eigenen Layer 2 Netz (VLAN) ohne DHCP
- Jool als Kernelmodul für NAT64

ipv6-mostly@home

- Raspberry Pi
- im eigenen Layer 2 Netz (VLAN) ohne DHCP
- Jool als Kernelmodul für NAT64
- Unbound als DNS64 (optional)
- geht auch mit `dns64.cloudflare-dns.com` oder `dns64.dns.google` im RA

ipv6-mostly@home

- Raspberry Pi
- im eigenen Layer 2 Netz (VLAN) ohne DHCP
- Jool als Kernelmodul für NAT64
- Unbound als DNS64 (optional)
- geht auch mit `dns64.cloudflare-dns.com` oder `dns64.dns.google` im RA
- systemd-networkd macht die RAs (alternativ RAdvd)

ipv6-mostly@home

- Raspberry Pi
- im eigenen Layer 2 Netz (VLAN) ohne DHCP
- Jool als Kernelmodul für NAT64
- Unbound als DNS64 (optional)
- geht auch mit `dns64.cloudflare-dns.com` oder `dns64.dns.google` im RA
- systemd-networkd macht die RAs (alternativ RAdvd)

```
$ ip -6 r
::1 dev lo proto kernel metric 30 pref medium
64:ff9b::/96 via fe80::ba27:ebff:fe89:fc2 dev Jannis-Network proto ra ↵
   metric 400 pref medium
2003:d8:123a:5401::/64 dev Jannis-Network proto ra metric 400 pref medium
fdba:48d0:bf0a:1::/64 dev Jannis-Network proto ra metric 400 pref medium
fe80::/64 dev Jannis-Network proto kernel metric 1024 pref medium
default via fe80::cea:14ff:fe87:7c4c dev Jannis-Network proto ra metric ↵
   400 pref high
```

Du hast noch kein IPv6?

- Prüfe mal deinen Router.

Du hast noch kein IPv6?

- Prüfe mal deinen Router.
- Überprüfe mal deinen ISP.

Du hast noch kein IPv6?

- Prüfe mal deinen Router.
- Überprüfe mal deinen ISP.
- Nutze einen Tunnel z.B. route64.org [6]
- route64 bietet auch Wireguard-Tunnel an. IPv6 hinter NAT möglich.

Du hast noch kein IPv6?

- Prüfe mal deinen Router.
- Überprüfe mal deinen ISP.
- Nutze einen Tunnel z.B. route64.org [6]
- route64 bietet auch Wireguard-Tunnel an. IPv6 hinter NAT möglich.
- Global wurde die 50% Marke an IPv6 Verbindungen geknackt (zu Google-Diensten) am 28.3.2026.
- In Deutschland sind es $>75\%$.

Fin

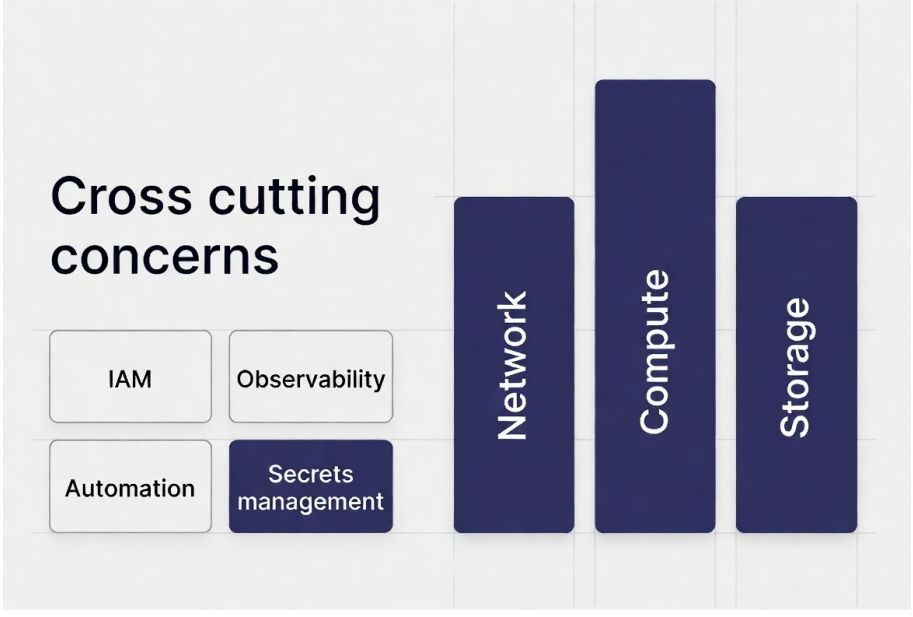
www.phoronix.com	**2606:4700:20::ac43:4b36**
a.pub.network	2606:4700:10::ac42:aa9f
ad-delivery.net	(no address)
c.pub.network	64:ff9b::34.160.152.31
cdn.ampproject.org	(no address)
cdn.privacy-mgmt.com	2600:9000:20e8:9600:1d:53f0:8080:93a1
d.pub.network	64:ff9b::34.160.152.31
dc8b551789d187eb0bd2a2a42∞ame.googlesyndication.com	2a00:1450:4001:c21::84
ep1.adtrafficquality.google	2a00:1450:4001:c17::9a
ep2.adtrafficquality.google	2a00:1450:4001:c25::84
fonts.googleapis.com	2a00:1450:4001:c13::5f
fonts.gstatic.com	2a00:1450:4001:c0f::5e
html-load.cc	2606:4700:10::6814:1801
pagead2.googlesyndication.com	2a00:1450:4001:c25::9d
region1.google-analytics.com	2001:4860:4802:32::36
s0.2mdn.net	2a00:1450:4001:c0f::94
securepubads.g.doubleclick.net	2a00:1450:4001:c15::9b
static.criteo.net	(no address)
tpc.googlesyndication.com	2a00:1450:4001:c1f::84
www.google-analytics.com	2a00:1450:4001:c17::71
www.google.com	2001:4860:4828:7700::
www.googletagmanager.com	2a00:1450:4001:c1f::61
www.gstatic.com	2a00:1450:4001:c17::5e
www.phoronix.net	2a06:98c1:3121::3

Abbildung: IPvFoo ist eine Browser-Erweiterung mit der sich die IP-Versionen beim Laden von Webseiten betrachten lassen

Quellen

- **Jool (NAT64)**: https://www.jool.mx/en/run-nat64.html
- **Unbound (DNS64)**: https://github.com/NLnetLabs/unbound/blob/master/doc/README.DNS64
- **TNAT64**: https://github.com/andrewshadura/tnat64
- **IPv6 Monostack**: https://ipv6.monostack.org
- **Coole Netzwerkvideos**: www.youtube.com/@apalrdsadventures
- **ROUTE64**: https://route64.org

Drei Säulen


Cross cutting concerns
IAM
Observability
Automation
Secrets management
Network
Compute
Storage

Resource PKI

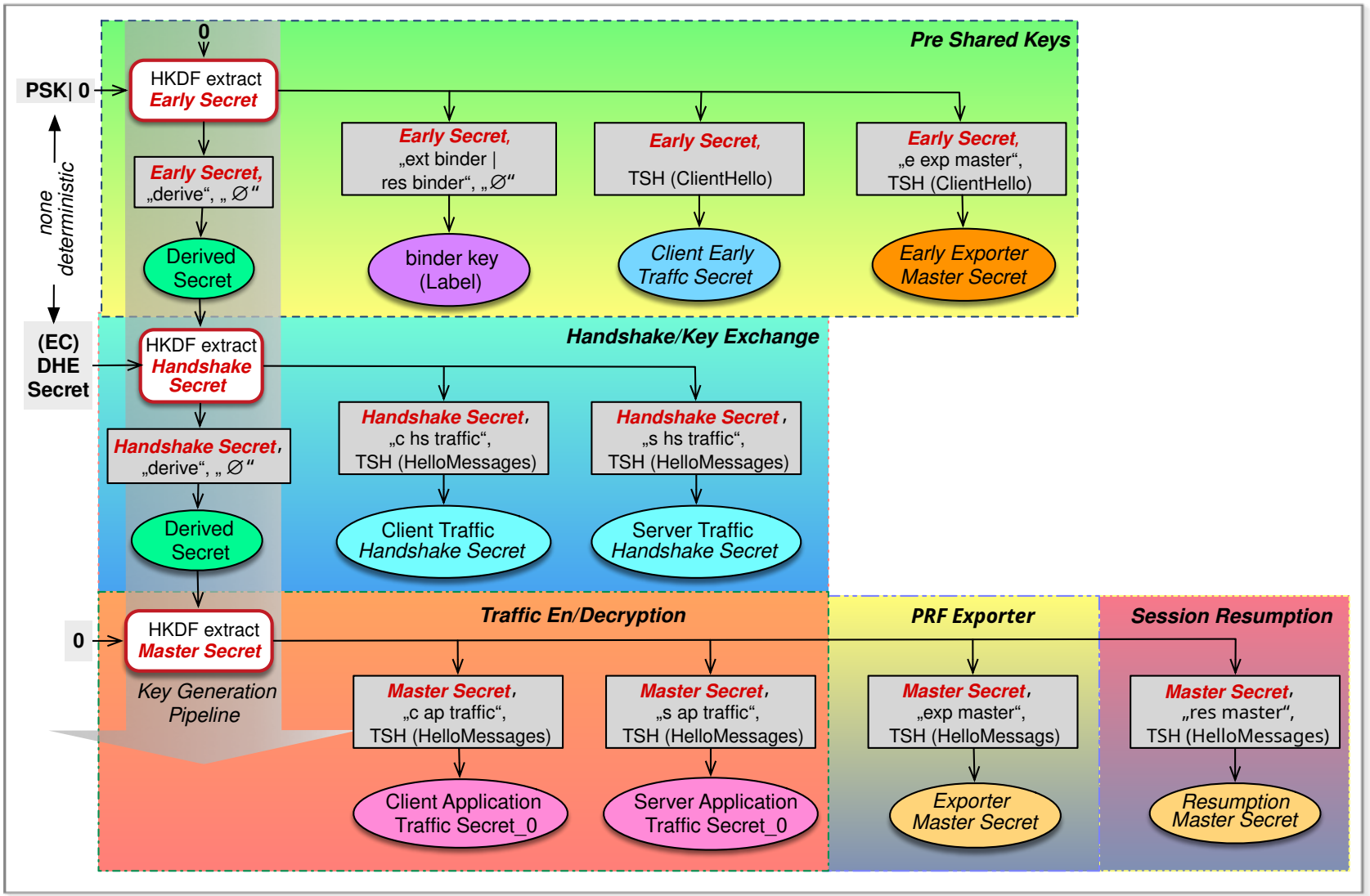
RPKI is (one of) the Internet's answers to that problem.

It works by letting the rightful owners of IP address blocks cryptographically sign a ROA; a small record that says: »IP prefix X is authorized to be announced by Autonomous System Number (ASN) Y.«

Routers that implement Route Origin Validation (ROV) then use those signed records to check incoming BGP announcements and drop the ones that don't match.

Quelle: `https://blog.apnic.net/2026/07/15/whos-running-all-those-tiny-rpki-servers/`

TLS Crypto Material und Usage



Quellen


RIPE92 Aufzeichnungen `https://ripe92.ripe.net/`


Technik der IP-Netze (MPLS, QUIC)
`https://www.hanser-fachbuch.de/Technik-der-IP-Netze/978-3-446-47371-3`


Zukunft der IP-Netze (SDN, IoT)
`https://www.hanser-fachbuch.de/Zukunft-der-IP-Netze/978-3-446-47756-8`


Broadband Integrated Services Digital Network (B-ISDN); B-ISDN Protocol Reference Model (PRM)
`https://www.etsi.org/deliver/etsi_i_ets/300300_300399/300354/01_60/ets_300354e01p.pdf`


D.J. Bernstein's Blog `https://blog.cr.yp.to/`


Sophie Schmieg's Blog (crypto, IETF TLS WG)
`https://keymaterial.net/author/sophieschmieg/`