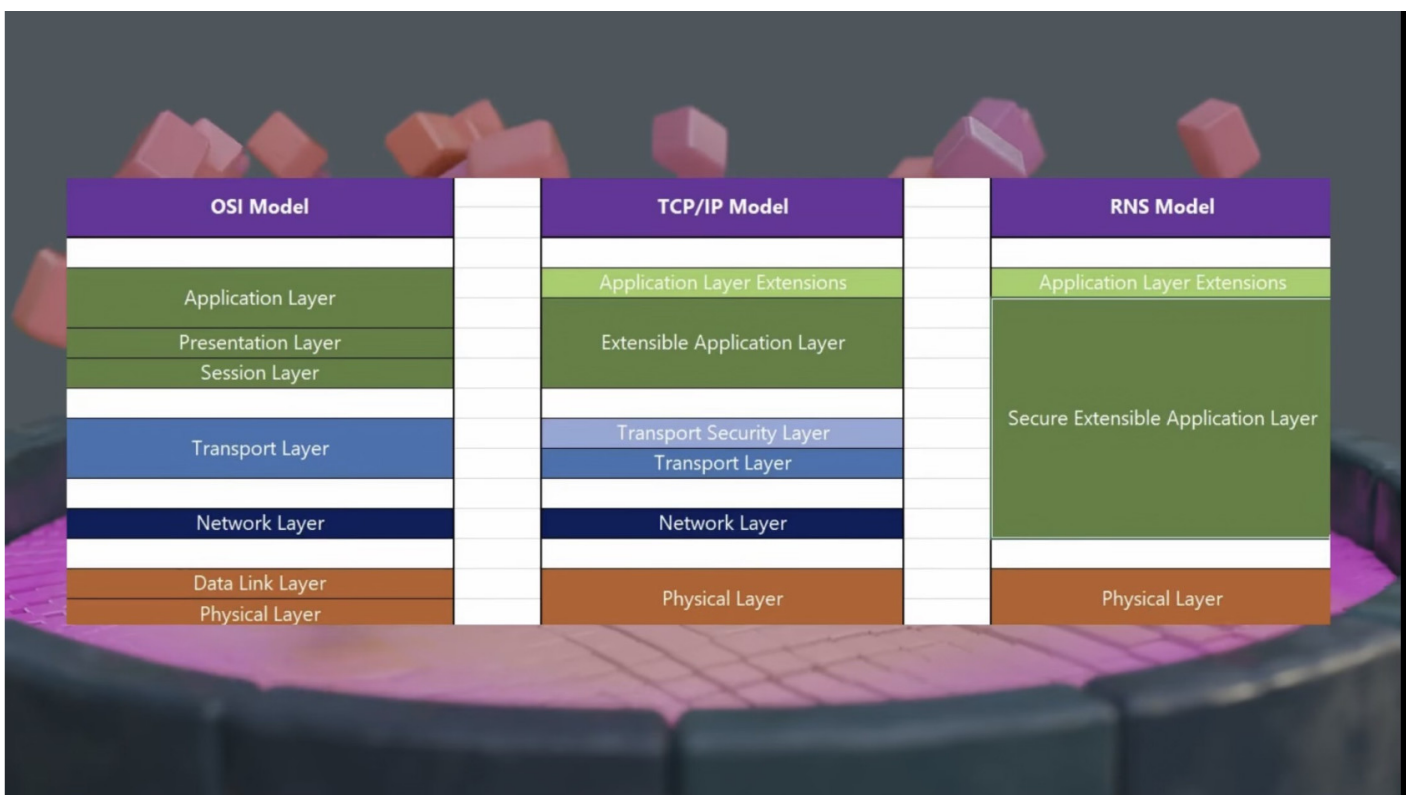


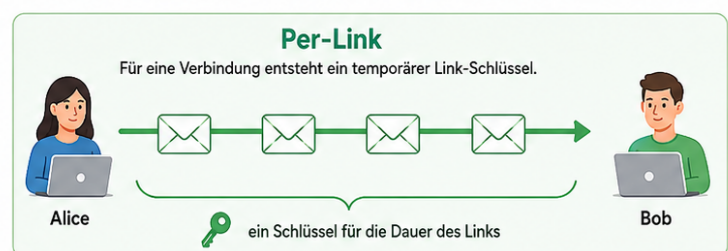
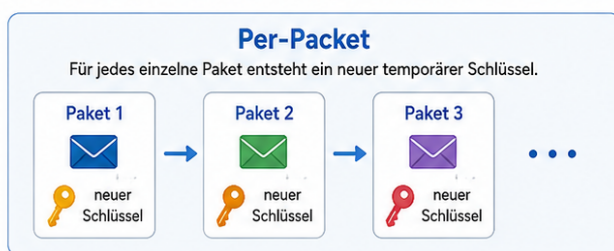
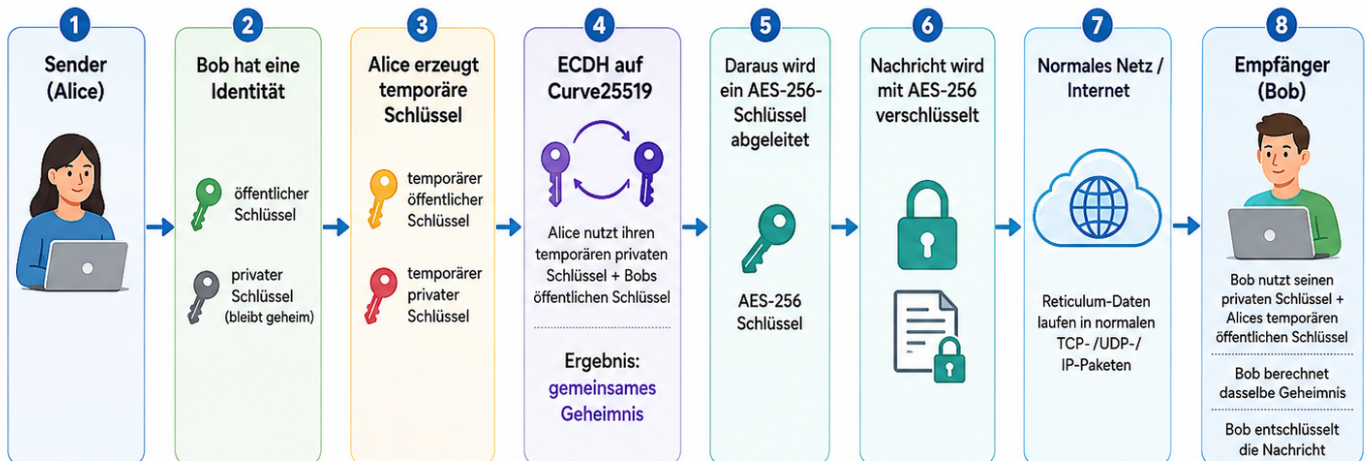
EXTRA: Reticulum Network Stack (RNS) im Vergleich zum OSI- und TCP/IP-Modell

“ **Hinweis:** Diese Seite ist ein Zukunfts-/Zusatzthema und gehört nicht zum klassischen IHK-Grundlagenstoff. Sie dient nur als technischer Blick darauf, wie moderne, dezentrale Netzwerk-Stacks wie Reticulum anders aufgebaut sein können als klassische Internet-Kommunikation.



Reticulum-Verschlüsselung einfach erklärt

Temporäre per-packet und per-link Schlüssel, ECDH auf Curve25519 und AES-256



Wichtig: Der private Schlüssel wird nie übertragen. Zwischenstationen leiten die Daten nur weiter, können den Inhalt aber nicht lesen.



Reticulum nutzt dauerhafte Identitäten + temporäre Schlüssel.

1. Grundidee

Das klassische **OSI-Modell** erklärt Netzwerkkommunikation in 7 Schichten:

1. Bitübertragungsschicht
2. Sicherungsschicht
3. Vermittlungsschicht
4. Transportschicht
5. Sitzungsschicht
6. Darstellungsschicht
7. Anwendungsschicht

Das **TCP/IP-Modell** ist praxisnäher und beschreibt grob, wie das heutige Internet funktioniert:

- Netzzugang / Physical + Link
- Internet Layer
- Transport Layer
- Application Layer

Das **RNS-Modell** von Reticulum denkt anders:



Reticulum ist kein einzelnes Protokoll wie TCP, IP oder TLS, sondern ein eigener Netzwerk-Stack, bei dem Identität, Routing, Transport und Verschlüsselung eng miteinander verbunden sind.

Reticulum kann über verschiedene darunterliegende Medien laufen, zum Beispiel:

- normales Internet
- TCP
- UDP
- WLAN
- Ethernet
- LoRa
- Packet Radio
- serielle Verbindungen
- I2P

Das vorhandene Medium ist dabei nur der Transportweg. Die eigentliche Reticulum-Kommunikation läuft darüber als eigenes kryptografisches Netzwerk.

2. Vergleich: OSI-Modell, TCP/IP-Modell und RNS-Modell

Bereich	OSI-Modell	TCP/IP-Modell	RNS / Reticulum
Anwendung	Application Layer	Application Layer	Application Layer Extensions
Darstellung	Presentation Layer	meist Teil der Anwendung	in Reticulum-Anwendungen integriert
Sitzung	Session Layer	meist Teil der Anwendung	durch Reticulum-Links und Sitzungslogik abgedeckt
Sicherheit	im OSI-Modell keine eigene Pflichtschicht	oft zusätzlich durch TLS, VPN oder App-Verschlüsselung	fest in Reticulum eingebaut
Transport	Transport Layer, z. B. TCP/UDP	Transport Layer, z. B. TCP/UDP	Reticulum übernimmt eigene Transport-/Link-Logik
Vermittlung / Routing	Network Layer, z. B. IP	Internet Layer, z. B. IP	kryptografisch gestützte Ziele, Pfade und Transport
Sicherung	Data Link Layer	Network Access / Link	abhängig vom verwendeten Medium
Physik	Physical Layer	Physical Layer / Network Access	Physical Layer / beliebiges Trägermedium

3. Was ist bei RNS anders?

Bei normalem Internetverkehr sieht der Ablauf stark vereinfacht so aus:

Schritt	Klassisches Internet
1	Eine Anwendung erzeugt Daten, z. B. Browser oder Messenger
2	TLS kann die Verbindung verschlüsseln
3	TCP sorgt für Transport und Reihenfolge
4	IP sorgt für Adressierung und Routing
5	Ethernet, WLAN oder Mobilfunk übertragen die Daten physisch

Bei Reticulum sieht die Denkweise anders aus:

Schritt	Reticulum / RNS
1	Eine Reticulum-Anwendung erzeugt Daten
2	Reticulum adressiert nicht klassisch nur über IP-Adressen, sondern über kryptografische Ziele
3	Reticulum verschlüsselt Inhalte standardmäßig Ende-zu-Ende
4	Reticulum kann temporäre Schlüssel pro Paket oder pro Link verwenden
5	Reticulum verpackt seine Daten in ein verfügbares Trägermedium
6	Dieses Trägermedium kann TCP, UDP, LoRa, Funk, seriell oder etwas anderes sein

4. Gegenüberstellung: Wie wird es bei RNS gemacht?

Aufgabe	Klassisch im OSI-/TCP/IP-Modell	Bei RNS / Reticulum
Adresse finden	IP-Adresse, DNS, Routingtabellen	kryptografische Identitäten und Destinations
Daten transportieren	TCP oder UDP	Reticulum-Pakete, Links und Transportlogik
Verbindung absichern	häufig TLS, VPN, IPsec oder App-Verschlüsselung	Verschlüsselung ist direkt Teil des Reticulum-Stacks
Identität prüfen	Zertifikate, DNS, CA, Login-Systeme	kryptografische Identität des Ziels

Aufgabe	Klassisch im OSI-/TCP/IP-Modell	Bei RNS / Reticulum
Daten über Internet senden	IP-Paket über Router	Reticulum-Paket wird in TCP/UDP/IP eingepackt
Daten über Funk senden	meist Spezialprotokoll nötig	Reticulum kann auch über LoRa, Packet Radio oder serielle Interfaces laufen
Zwischenstationen	Router sehen IP-Adressen und leiten weiter	Reticulum-Knoten leiten Pakete weiter, ohne den Inhalt lesen zu können
Anwendungsschicht	HTTP, SMTP, DNS, Messenger-Protokolle	Reticulum-Anwendungen oder Erweiterungen, z. B. Messaging über LXMf
Verschlüsselung	oft Zusatzschicht über TCP/IP	eingebauter Bestandteil des Netzwerks
Abhängigkeit vom Internet	meist stark abhängig von IP-Infrastruktur	kann IP nutzen, ist aber nicht grundsätzlich davon abhängig

5. Erklärung anhand der Grafik

Die Grafik vergleicht drei Modelle:

Modell	Bedeutung
OSI-Modell	theoretisches 7-Schichten-Modell zur Erklärung von Netzwerkkommunikation
TCP/IP-Modell	praxisnahes Modell des heutigen Internets
RNS-Modell	Reticulum Network Stack als kryptografiebasierter Netzwerk-Stack

Im OSI-Modell sind die Aufgaben stark aufgeteilt:

- Anwendung
- Darstellung
- Sitzung
- Transport
- Netzwerk
- Sicherung
- Physik

Im TCP/IP-Modell werden mehrere OSI-Schichten zusammengefasst:

- Anwendung
- Transport
- Netzwerk

- Physik/Link

Im RNS-Modell wird vieles noch stärker zusammengeführt:

- Application Layer Extensions
- Secure Extensible Application Layer
- Physical Layer

Das bedeutet:

“ Reticulum legt sehr viele Funktionen, die sonst auf mehrere Schichten verteilt sind, in eine sichere und erweiterbare Reticulum-Schicht.

Diese Reticulum-Schicht übernimmt dann unter anderem:

- kryptografische Identität
- sichere Ziele
- Paketverschlüsselung
- Link-Aufbau
- Weiterleitung über mehrere Knoten
- Transport über unterschiedliche Medien
- Nutzung von TCP/UDP/IP als möglicher Träger
- Nutzung von Funk, LoRa oder seriellen Verbindungen als möglicher Träger

6. Beispiel: Reticulum über normales Internet

Reticulum kann über das bestehende Internet laufen.

Dabei wird nicht das normale IP-Paketformat verändert. Stattdessen wird ein Reticulum-Paket in ein normales TCP- oder UDP-Paket eingepackt.

Zusatz: Welche Rolle spielt DNS bei Reticulum?

Wenn Reticulum über das normale Internet läuft, kann DNS trotzdem vorkommen. DNS ist dann aber **nicht** dafür zuständig, den eigentlichen Reticulum-Empfänger zu finden.

DNS macht nur das, was DNS im klassischen Internet immer macht:

Domainname

↓

IP-Adresse

Beispiel:

```
reticulum-node.example.org
↓
203.0.113.10
```

Damit findet der Rechner zunächst nur einen bekannten Reticulum-Knoten im normalen Internet.

Der eigentliche Reticulum-Weg sieht vereinfacht so aus:

```
Alice / Reticulum-App
↓
DNS löst eventuell einen Einstiegsknoten auf
↓
normales Internet bringt das Paket zu diesem Reticulum-Knoten
↓
ab dort übernimmt Reticulum selbst
↓
Reticulum sucht das Ziel über Destinations und Announcements
↓
Paket wird über Reticulum-Knoten weitergeleitet
↓
Bob / Reticulum-Ziel empfängt und entschlüsselt
```

Wichtig ist also:

“ DNS kennt höchstens den Einstiegspunkt ins Reticulum-Netz, aber nicht automatisch den endgültigen Reticulum-Empfänger.

Der normale Internet-Router sieht nur:

```
IP A sendet TCP-/UDP-Daten an IP B
```

Er sieht aber nicht:

```
Dieses Reticulum-Paket ist für Bob.
Das ist Bobs Reticulum-Destination.
```

Das ist der Inhalt der Nachricht.

Reticulum selbst arbeitet nicht hauptsächlich mit Domains oder klassischen IP-Zieladressen, sondern mit kryptografischen Zielen, sogenannten **Destinations**.

Vereinfacht:

Aufgabe	Klassisches Internet	Reticulum
Namen auflösen	DNS macht aus Domain eine IP-Adresse	DNS höchstens für Einstiegsknoten nötig
Ziel finden	IP-Adresse / Domain	Reticulum-Destination
Weiterleitung	IP-Router leiten anhand der Ziel-IP weiter	Reticulum-Knoten leiten anhand bekannter Pfade zu Destinations weiter
Herkunft im Paket	IP-Pakete enthalten normalerweise eine Quell-IP	Reticulum-Pakete enthalten keine klassische Quelladresse
Inhalt lesen	nur geschützt, wenn z. B. TLS genutzt wird	Reticulum-Inhalt ist Ende-zu-Ende verschlüsselt

Reticulum-Knoten lernen erreichbare Ziele über sogenannte **Announcements**. Wenn ein Ziel im Reticulum-Netz angekündigt wird, merken sich andere Reticulum-Knoten, über welchen Nachbarn dieses Ziel erreichbar ist. Später können sie Pakete in diese Richtung weiterleiten.

Merksatz:

“ DNS bringt dich bei Reticulum über das Internet höchstens bis zu einem bekannten Reticulum-Knoten. Danach übernimmt Reticulum selbst mit kryptografischen Destinations, Announcements und eigener Weiterleitung. Normale Internet-Router transportieren dabei nur TCP-/UDP-/IP-Pakete, verstehen aber den Reticulum-Inhalt nicht.

Ablauf:

Schritt	Beschreibung
1	Eine Reticulum-Anwendung erstellt eine Nachricht
2	Reticulum verschlüsselt die Nachricht
3	Reticulum erzeugt ein eigenes Reticulum-Paket
4	Dieses Paket wird in TCP oder UDP eingepackt
5	TCP/UDP läuft wie gewohnt über IP

Schritt	Beschreibung
6	Normale Router leiten das Paket weiter
7	Der Empfänger entpackt das Reticulum-Paket
8	Reticulum entschlüsselt die Nachricht beim richtigen Empfänger

Vereinfacht:

Reticulum-Nachricht

↓

Reticulum-Verschlüsselung

↓

Reticulum-Paket

↓

TCP/UDP-Paket

↓

IP-Paket

↓

Internet

↓

Empfänger entschlüsselt Reticulum-Nachricht

7. Warum braucht RNS nicht zwingend IP?

Im klassischen Internet ist IP die zentrale Vermittlungsschicht.

Bei Reticulum ist das anders:

“ Reticulum kann IP benutzen, muss es aber nicht.

Das heißt:

Situation	Reticulum-Nutzung
normales Heimnetz	Reticulum kann über TCP/UDP/IP laufen
Internet	Reticulum kann über TCP/UDP/IP getunnelt werden
LoRa-Funk	Reticulum kann direkt über LoRa laufen
Packet Radio	Reticulum kann über Funkmodems laufen
serielle Verbindung	Reticulum kann über serielle Schnittstellen laufen
I2P	Reticulum kann über ein anonymisierendes Overlay laufen

Deshalb ist Reticulum besonders interessant für Netze, die nicht immer wie normales Internet funktionieren.

Zum Beispiel:

- Notfallkommunikation
- Mesh-Netze
- Funknetze
- LoRa-Kommunikation
- dezentrale Kommunikation
- Kommunikation mit sehr niedriger Bandbreite
- Kommunikation bei hoher Latenz
- Netze ohne zentrale Infrastruktur

8. Was bedeutet „Secure Extensible Application Layer“?

In der Grafik ist beim RNS-Modell eine große grüne Schicht zu sehen:

Secure Extensible Application Layer

Das bedeutet vereinfacht:

“ Reticulum stellt eine sichere, erweiterbare Kommunikationsschicht bereit, auf der Anwendungen aufbauen können.

Diese Schicht ersetzt nicht einfach nur eine einzelne OSI-Schicht. Sie übernimmt mehrere Aufgaben gleichzeitig.

Klassische Aufgabe	Bei RNS ungefähr enthalten in
Adressierung	Secure Extensible Application Layer
Routing / Weiterleitung	Secure Extensible Application Layer
Verschlüsselung	Secure Extensible Application Layer
Sitzungs-/Link-Aufbau	Secure Extensible Application Layer
Pakettransport	Secure Extensible Application Layer
Anwendungserweiterungen	Application Layer Extensions

Dadurch wirkt RNS im Vergleich zum OSI-Modell viel kompakter.

9. Wichtiger Unterschied zu TLS/HTTPS

TLS/HTTPS funktioniert normalerweise so:

Ebene	Klassisches HTTPS
Anwendung	Browser / Webserver
Sicherheit	TLS
Transport	TCP
Netzwerk	IP
Physik	Ethernet, WLAN, Mobilfunk

Reticulum funktioniert eher so:

Ebene	Reticulum
Anwendung	Reticulum-App
Sicherheit	direkt in Reticulum
Transportlogik	direkt in Reticulum
Routing/Ziele	direkt in Reticulum
Trägermedium	TCP, UDP, LoRa, Funk, seriell, WLAN usw.

Merksatz:

“ TLS schützt eine bestehende TCP/IP-Verbindung. Reticulum baut ein eigenes kryptografisches Netzwerk, das TCP/IP nur als eine mögliche Transportmöglichkeit verwenden kann.

10. Kurze Lernzusammenfassung

Reticulum / RNS unterscheidet sich vom OSI- und TCP/IP-Modell vor allem dadurch, dass es nicht einfach eine weitere Verschlüsselungsschicht über das Internet legt.

Stattdessen ist Reticulum ein eigener Netzwerk-Stack.

Er verbindet:

- Identität
- Adressierung
- Verschlüsselung
- Transport
- Routing
- Anwendungserweiterungen

in einem kryptografisch aufgebauten System.

Das normale Internet kann dabei weiterhin benutzt werden, ist aber nur ein möglicher Transportweg.

Reticulum kann deshalb über TCP/UDP/IP laufen, aber auch über LoRa, Funk, serielle Verbindungen oder andere Medien.

11. Merksatz

“ Das OSI-Modell trennt Netzwerkkommunikation in viele einzelne Schichten. TCP/IP setzt diese Idee praxisnah für das Internet um. RNS/Reticulum geht einen anderen Weg: Es baut ein eigenes kryptografisches Netzwerk, in dem Sicherheit, Identität, Routing und Transport direkt zusammengehören. Das darunterliegende Medium kann normales Internet sein, muss es aber nicht.

12. Mini-Vergleich für den Kopf

Frage	OSI / TCP/IP	RNS / Reticulum
Braucht es IP?	meistens ja	nein, aber IP kann genutzt werden
Ist Verschlüsselung automatisch Teil des Modells?	nein, meist Zusatz wie TLS/VPN	ja, zentraler Bestandteil
Für normales Web geeignet?	ja	nicht als direkter Ersatz für normales Web gedacht
Für Mesh/Funk/LoRa geeignet?	nur mit Zusatzlösungen	genau dafür interessant
Müssen Router Reticulum verstehen?	nur Reticulum-Knoten müssen es verstehen	normale IP-Router leiten nur TCP/UDP weiter
Können Zwischenstationen Inhalte lesen?	abhängig von Verschlüsselung	bei verschlüsselter Reticulum-Kommunikation nein
Hauptidee	standardisierte Schichten	kryptografisches dezentrales Netzwerk

13. Abschluss-Merksatz

“ Reticulum kann das bestehende Internet als Transportweg nutzen, ersetzt es aber nicht einfach. Das klassische Internet bleibt für Web, Browser, Streaming,

Cloud und Apps praktischer. Reticulum ist dagegen besonders stark bei dezentraler, sicherer und robuster Kommunikation – vor allem bei Mesh, Funk, LoRa, hoher Latenz, wenig Bandbreite und autonomen Netzen.

Quellen / weiterführende Links

- Reticulum Manual: <https://reticulum.network/manual/>
- What is Reticulum?: <https://reticulum.network/manual/whatis.html>
- Understanding Reticulum: <https://reticulum.network/manual/understanding.html>
- Cryptographic Primitives: <https://reticulum.network/crypto.html>
- GitHub-Projekt: <https://github.com/markqvist/Reticulum>

Revision #14

Created 3 June 2026 10:53:05 by Admin

Updated 3 June 2026 12:36:44 by Admin