1-RTT (One Round Trip Time)

1-RTT je termín používaný v síťové komunikaci k popisu latence při navazování spojení. Označuje situaci, kdy klient a server potřebují pouze **jeden kompletní cyklus** (jeden dotaz a jednu odpověď), aby se dohodli na šifrovacích klíčích a mohli začít posílat užitečná data (HTTP data).

Toto vylepšení přinesl protokol **TLS 1.3** a představuje zásadní zrychlení oproti staršímu TLS 1.2.

Srovnání latence při navazování spojení

Doba navázání spojení (handshake) se výrazně liší podle verze protokolu:

TLS 1.2 (2-RTT)

Ve starší verzi musel proběhnout handshake ve dvou krocích:

```
1. **RTT 1:** Výměna informací o schopnostech a algoritmech (Client Hello / Server Hello).
2. **RTT 2:** Výměna klíčů a potvrzení šifrování.
```

Teprve po druhém cyklu mohl klient poslat např. požadavek na zobrazení stránky.

TLS 1.3 (1-RTT)

V nové verzi klient **předpokládá** nejmodernější sadu šifer a posílá svůj podíl pro výměnu klíčů (Key Share) hned v první zprávě.

```
1. **RTT 1:** Klient pošle nabídku i klíče -> Server odpoví svými klíči a certifikátem.
```

Ihned poté (v rámci téhož cyklu) může následovat přenos šifrovaných dat.

Proč je 1-RTT důležité?

- **Rychlost načítání:** Snižuje viditelnou latenci při prvním přístupu na web, což je kritické zejména pro mobilní sítě s vysokou odezvou (ping).
- **Uživatelská zkušenost:** Čas „Time to First Byte“ (TTFB) je díky 1-RTT mnohem nižší.
- **Efektivita:** Méně zpráv v síti znamená menší režii pro síťová zařízení.

Extrémní případ: 0-RTT (Zero Round Trip Time)

TLS 1.3 podporuje také režim **0-RTT** (také známý jako **TLS Resumption**). Pokud se klient k danému serveru již dříve připojil:

- Klient může poslat šifrovaná data (např. HTTP GET) hned v **prvním paketu**, aniž by čekal na jakoukoliv odpověď ze serveru.
- **Riziko:** Tento režim je náchylný k tzv. *Replay Attacks* (útokům opakováním), proto se používá jen pro specifické typy požadavků.

Srovnání v tabulce

Protokol	Počet RTT	Poznámka
TCP Handshake	1 RTT	Základní navázání spojení (SYN/ACK).
TLS 1.2	**2 RTT**	Pomalé, mnoho zpráv tam a zpět.
TLS 1.3	**1 RTT**	Moderní standard, rychlý a bezpečný.
QUIC / HTTP/3	**0-1 RTT**	Spojuje TCP a TLS handshake do jednoho kroku.

> **Zajímavost:** Při komunikaci se serverem na druhém konci světa (latence např. 200 ms) znamená rozdíl mezi 2-RTT a 1-RTT úsporu celých 200 ms jen při samotném připojování.

— **Viz také:** HTTPS/TLS, TCP Protocol, Síťová latence