PANORAMICA SUI PROTOCOLLI DI TRASPORTO MENO CONOSCIUTI

Durante il corso di Computer Network sono stati trattati i principali protocolli di trasporto: TCP e UDP. Tuttavia ne esistono molti altri che derivano da questi ultimi e che combinano alcune delle loro caratteristiche.

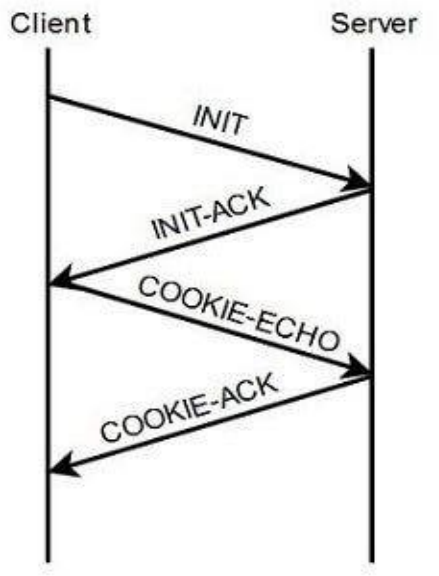

Figura 1. Impostazione della connessione STCP

Uno di questi è l'STCP (Stream Transmission Control Protocol), sviluppato dall'IETF e pubblicato nel 2000: è orientato alla connessione e si contraddistingue per tipo di trasmissione orientata ai messaggi, per tolleranza ai guasti e per la consegna dei dati parzialmente ordinata.

I principali vantaggi consistono nella consegna dei dati attraverso flussi indipendenti; l'ordine dei dati all'interno del flusso viene rispettato in maniera rigorosa, mentre non è stabilito nessun ordinamento per la consegna dei flussi.

La connessione viene stabilita attraverso un 4-way handshake - "stretta di mano a quattro vie" - in modo tale da non essere vulnerabile agli attacchi flooding (negazione del servizio tramite il consumo di banda che ostruisce la rete).

STCP supporta anche il multi-homing: quando uno o entrambi

gli endpoint possiedono più di un indirizzo IP, ogni host stabilisce un indirizzo principale a cui inviare i dati, mentre gli altri eventuali indirizzi vengono utilizzati per avere ridondanza. Vi è quindi una maggiore tolleranza degli errori avendo più indirizzi di rete validi. Per questo motivo è stata implementata una gestione dei percorsi che ne controlla la disponibilità inviando in maniera regolare degli heartbeat (segnali di controllo).

L'STCP somiglia dunque al TCP per l'affidabilità, l'orientamento alla connessione, la gestione del flusso, il controllo della congestione, e all'UDP, da cui eredita l'orientamento al messaggio e l'utilizzo nelle applicazioni real-time.

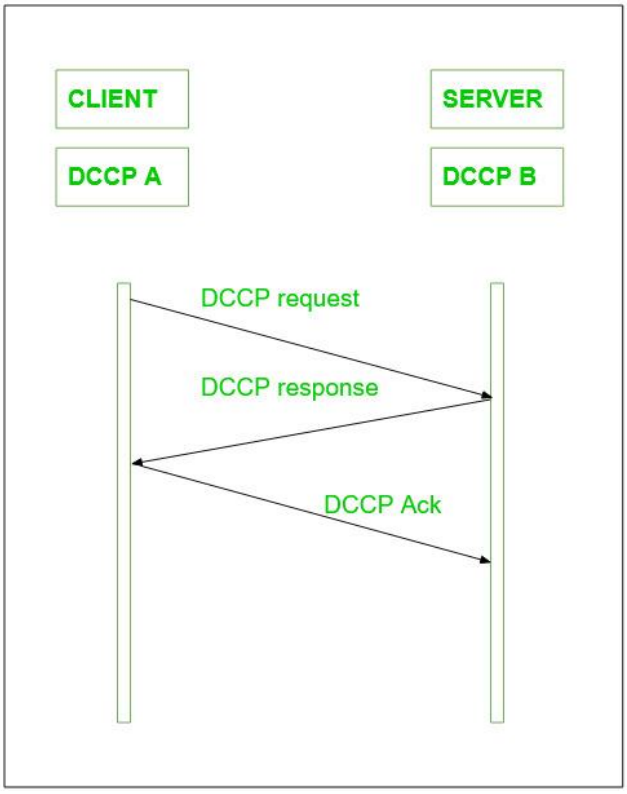

Figura 2. Impostazione della connessione DCCP

Il DCCP (Datagram Congestion Control Protocol) viene invece sviluppato nel 2006 dall'IETF con lo scopo di favorire il controllo della congestione senza la necessità di implementazione a livello applicativo.
Il flusso di traffico contiene messaggi di conferma (Explicit Congestion Notification), trasmessi in modo completamente affidabile, mentre la consegna in sequenza all'interno dei flussi non è disponibile.
I vecchi messaggi, come nello UDP, diventano rapidamente inutili: si preferisce infatti la trasmissione veloce dei messaggi piuttosto che la loro ritrasmissione.
Il DCCP viene usato come tecnica di controllo della congestione per le applicazioni che fanno uso dell'UDP, infatti regola dinamicamente la velocità di invio dei dati in base alla congestione della rete. Se un nodo rileva congestione, attraverso segnali come la perdita di pacchetti o la latenza elevata, il DCCP può ridurre la velocità di trasmissione per evitare il sovraccarico della rete;
fornisce inoltre un feedback continuo sullo stato di congestione attraverso i messaggi di acknowledgment.
Il DCCP consente inoltre di stabilire la priorità dei flussi dati ed è in grado di supportare più flussi contemporanei all'interno di un'unica connessione.
Questo protocollo viene usato anche per la sua compatibilità (come tra reti IPv4 e reti IPv6) e per la sua flessibilità, supportando sia la modalità di comunicazione orientata alla connessione, sia quella senza connessione.
Il DCCP viene utilizzato per applicazioni che hanno vincoli di temporizzazione sulla consegna dei dati, ad esempio la telefonia internet, le applicazioni di streaming, i giochi online multigiocatore e la telemetria (tecnologia che permette la misurazione e la trascrizione di informazioni utili al progettista di sistema).

Il RUDP (Reliable User Datagram Protocol) è stato progettato per fornire una soluzione più affidabile dell'UDP: la consegna dei pacchetti avviene in ordine garantito e la qualità del servizio risulta più performante ma meno complessa e sovraccaricata rispetto al TCP.

Le funzionalità che vengono implementate sono il riconoscimento dei pacchetti vuoti, il controllo di flusso, la ritrasmissione dei pacchetti persi, il buffering e il protocollo a finestra scorrevole (sliding window),
infatti una dimensione della finestra viene sempre mantenuta libera sia dal mittente che dal destinatario.
I buffer condivisi vengono sincronizzati mediante semafori di conteggio così che un thread per volta possa accedere al buffer.
Due variabili, base e next, mantengono traccia della finestra funzionante: quando il mittente invia un pacchetto, la variabile successiva viene incrementata, così da poter calcolare il numero di pacchetti nel buffer.
Il RUDP trova applicazione in VoIP, videochiamate, videoconferenze, streaming multimediale, giochi online in tempo reale, IoT e trasmissione di dati sensibili alla latenza (ad esempio il trading finanziario).
Il RUDP è quindi ideale per applicazioni che necessitano di una trasmissione rapida e attendibile, ma che non richiedono la garanzia assoluta di consegna di ogni pacchetto, permettendo così di ridurre la latenza e ottimizzare l'esperienza utente.

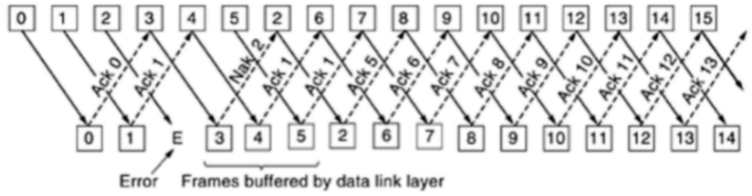

Figure 4. The architecture of RUDP.

Figura 3. Schema di invio pacchetti del RUDP

	TCP	RUDP	UDP
Packets transmitted	5833.2	5833.2	5833.2
Packets received	5833.2	5824.8	5749.8
Success rate	100%	99.8%	98.5%

Table 2. Number of Received Packets.

Figura 4. Test effettuato usando TCP, RUDP e UDP

Il QUIC (Quick UDP Internet Connections) è stato progettato da Jim Roskind (Google) e distribuito nel 2012: viene sviluppato per il suo impiego in applicazioni web che implementano l'HTTP/3 su dispositivi mobili. Non è ancora una versione ufficiale, ma è già utilizzato da più del 50% di tutte le connessioni Chrome ai server Google.
QUIC fonde UDP e TCP: pur essendo basato su UDP, nel QUIC vi è un handshake. Quando viene stabilita la prima connessione tra client e server (1-RTT),
il client memorizza le informazioni del server per le connessioni successive, in modo da dover usare un solo pacchetto per l'avvio della successiva connessione con lo stesso server (0-RTT). Ciò comporta un miglioramento dei tempi di connessione e caricamento, oltre ad una sicurezza maggiore rispetto al TCP, infatti viene utilizzato il TLS 1.3 per la crittografia.
Altri vantaggi consistono nel miglioramento delle prestazioni durante i cambi di rete (ad esempio passando da una rete mobile al Wi-Fi), nell'opzione di multiplexing (tecnica utilizzata per combinare più flussi di dati contemporaneamente in un unico canale di trasmissione), nell'uso del Packet Pacing (limitazione automatica della trasmissione dei pacchetti, che vengono inviati distribuiti nel tempo invece che in blocchi) e nella sua indipendenza dall'hardware.
A suo sfavore vi è invece un'intestazione con meno informazioni in chiaro che rende più onerosa la risoluzione di errori, il supporto limitato e l'incompatibilità con alcuni vecchi dispositivi.
Nonostante sia ancora una versione provvisoria, già dal 2013 molti siti web implementano questo protocollo, come i prodotti Google, YouTube e Facebook.

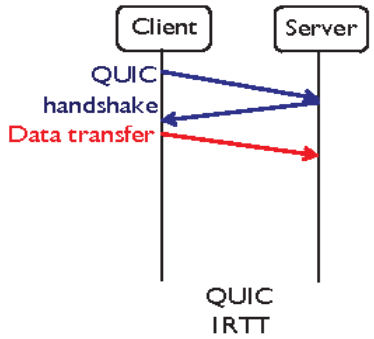

Figura 5. 1-RTT handshake

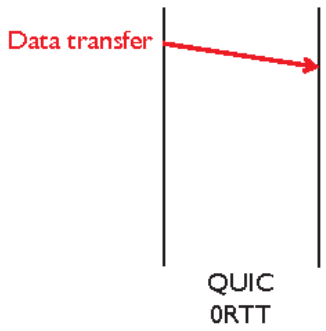

Figura 6. 0-RTT handshake

Il GRE (Generic Routing Encapsulation) è stato progettato nel 1994 come strumento di tunneling.
È in grado di incapsulare fino a venti tipi di protocolli diversi sopra una rete IP, così che i pacchetti possano viaggiare tra due protocolli o reti incompatibili (utile in caso di conversione da IPv4 a IPv6 e viceversa).
La creazione di un tunnel comporta la creazione di un pacchetto GRE che avrà due intestazioni IP: quella originale da 20 bytes e una nuova intestazione di 4 bytes che indica il tipo e l'identificativo di protocollo usato dal pacchetto incapsulato, gli indirizzi di origine e destinazione e il numero di sequenza.
Dopo che viene stabilita una connessione virtuale point-to-point, il pacchetto viene spedito nel tunnel, raggiungendo il router di destinazione. L'intestazione GRE viene rimossa (decapsulazione) e il payload viene dato in carico al protocollo nativo della LAN in cui giunge.
Questi tipi di tunnel vengono definiti "stateless": ciò significa che i routers non conservano informazioni (stato, disponibilità) sui routers riceventi.
I vantaggi del GRE sono l'operabilità delle VPN sulle reti WAN, il collegamento delle sottoreti discontinue, il loro utilizzo nelle reti con hops limitati tra routers e il raggruppamento di più protocolli sotto uno solo.
Lo svantaggio principale è che non viene considerato un protocollo sicuro poiché non utilizza la crittografia IPsec, rendendosi vulnerabile agli attacchi DDoS (intasamento della rete che ne causa l'inaccessibilità).

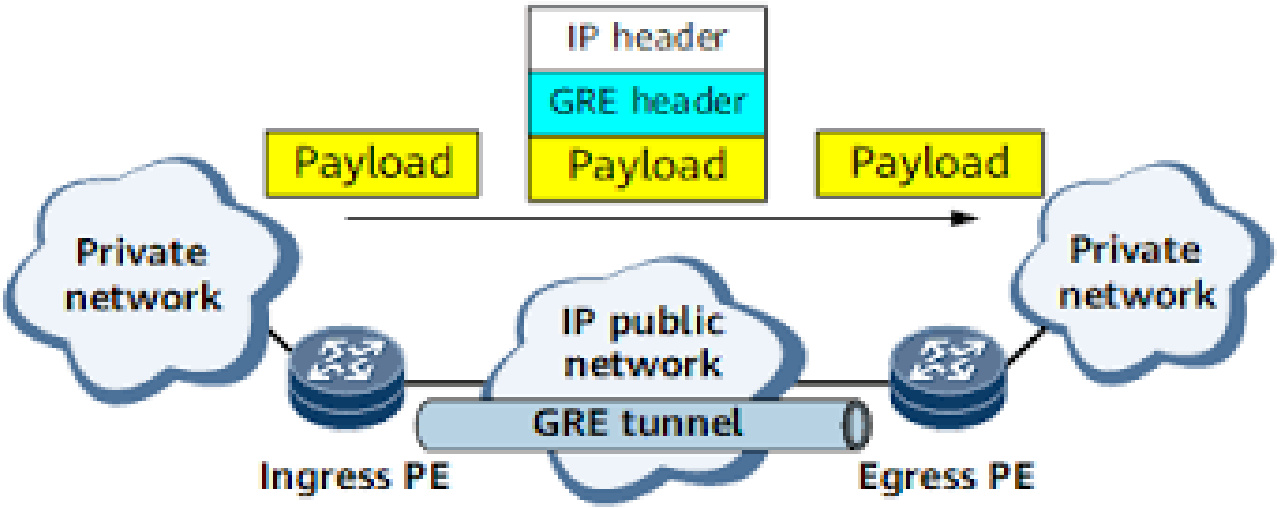

Figura 7. Schema degli headers nel tunnel GRE

L'MPTCP (Multi Path Transmission Control Protocol), pubblicato nel 2013 dall'IETF, è stato progettato per consentire una connessione TCP che riesca a migliorare la produttività: utilizza più percorsi e aumenta la ridondanza, grazie alla quale è possibile usare il multiplexing (come nel QUIC).
Viene principalmente usato nelle reti wireless: i collegamenti possono essere aggiunti o eliminati quando l'utente si sposta all'interno o all'esterno della copertura senza interrompere la connessione TCP.
Uno dei vantaggi dell'MPTCP è il miglioramento delle prestazioni dei data center a causa del throughput (velocità di trasmissione dei dati) molto elevato, mentre il principale svantaggio è l'inefficienza dei firewall: poiché sono utilizzati più flussi di dati contemporaneamente, il traffico di rete diventa più complesso da monitorare. I firewalls devono poter infatti comprendere come i vari flussi siano correlati tra loro, identificando tutte le sottoconnessioni appartenenti alla stessa sessione TCP.
In particolare, Apple si serve dell'MPTCP per supportare Siri su Iphone, dove si ottiene un feedback dell'utente più veloce e una notevole riduzione dei guasti di rete.

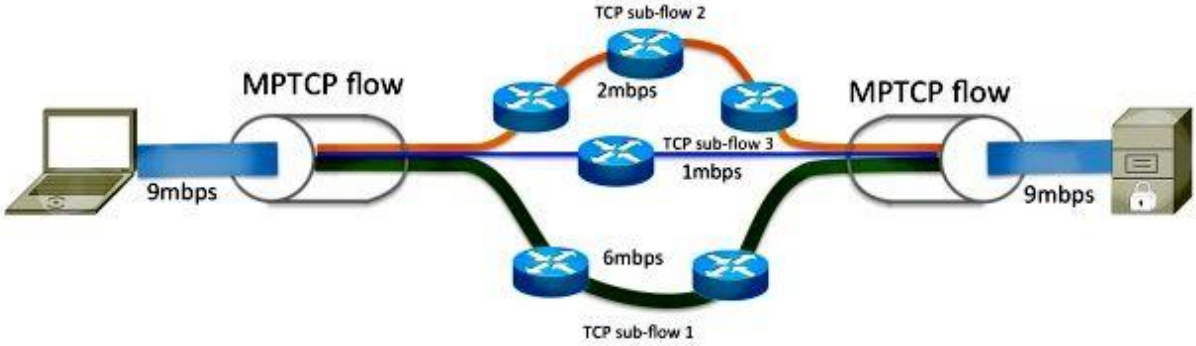

Figura 8. Schema dell'architettura MPTCP

Per riassumere, In termini di affidabilità, QUIC, MPTCP e STCP offrono alte prestazioni, mentre DCCP e RUDP si collocano ad un livello intermedio.
Il GRE, non utilizzando la crittografia ed essendo un protocollo di tunneling senza gestione della congestione, ha invece una bassa affidabilità.
DCCP, MPTCP e STCP hanno più similitudini con il TCP, il RUDP si avvicina maggiormente all'UDP, mentre il QUIC si colloca nel mezzo.
In conclusione, la varietà di applicazioni e servizi moderni non può essere facilmente categorizzata nel solo uso di TCP o UDP, per questo motivo l'utilizzo di uno di questi protocolli "minori" è spesso la soluzione migliore, che trova il giusto compromesso tra velocità e attendibilità.

Di seguito una tabella riassuntiva delle principali caratteristiche.

Protocollo	Affidabilità	Connessione	Gestione della Congestione	Similitudine con
STCP	Alta	4 way handshake	Gestione della congestione (ottimizzata per la latenza)	Più simile a TCP
DCCP	Media (opzionale)	Connection Oriented / Connectionless	Controllo della congestione esplicito (supporta vari algoritmi)	Più simile a TCP
RUDP	Media (opzionale)	3 way handshake	Controllo della congestione (senza la pesantezza di TCP)	Più simile a UDP
GRE	Nessuna affidabilità	Nessuna connessione	Nessun controllo della congestione	Protocollo di tunneling
QUIC	Alta	1-RTT handshake o 0-RTT handshake	Gestione della congestione (basata su TCP, ma ottimizzata per la latenza)	Fusione tra TCP e UDP
MPTCP	Alta	3 way handshake	Controllo della congestione (su più path)	Più simile a TCP

SITOGRAFIA E FONTI ICONOGRAFICHE:

STCP
https://www.ibm.com/docs/it/aix/7.3?topic=protocol-stream-control-transmission
https://www.ionos.it/digitalguide/server/know-how/sctp/
https://datatracker.ietf.org/doc/html/draft-burleigh-dtn-stcp-00
DCCP
https://ieeexplore.ieee.org/document/6479592
https://www.geeksforgeeks.org/what-is-dccp-datagram-congestion-control-protocol/
https://datatracker.ietf.org/doc/html/rfc4340
RUDP
https://www.geeksforgeeks.org/reliable-user-datagram-protocol-rudp/
https://datatracker.ietf.org/doc/html/draft-ietf-sigtran-reliable-udp-00
https://www.semanticscholar.org/paper/Reliable-User-Datagram-Protocol-as-a-Solution-to-in-Huh/68abd653d1aaa2570d07aa5c267b173ff5164e78
QUIC
https://www.ionos.it/digitalguide/hosting/tecniche-hosting/quic-il-protocollo-di-trasporto-dati-basato-su-udp/
https://datatracker.ietf.org/doc/rfc9000/
https://www.coretech.it/it/service/knowledge_base/Sicurezza/Sviluppo-Sicuro/Il-protocollo-HTTP3-e-Quic.php
https://www.semanticscholar.org/paper/Innovating-Transport-with-QUIC%3A-Design-Approaches-Cui-Li/79486a663f7bc3f489b25b99bd90bde3bdaadb6b
GRE
https://www.techtarget.com/searchnetworking/definition/Generic-Routing-Encapsulation-GRE
https://datatracker.ietf.org/doc/rfc2784/
https://datatracker.ietf.org/doc/html/rfc1701
https://info.support.huawei.com/info-finder/encyclopedia/en/GRE.html
MPTCP
https://www.cisco.com/c/it_it/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
https://www.redhat.com/en/blog/understanding-multipath-tcp-networking-highway-future
https://datatracker.ietf.org/doc/rfc8684/
https://datatracker.ietf.org/doc/html/rfc8684