1 Introduzione

La rete può essere vista come un insieme di terminali, collegamenti e nodi, che utilizzano varie tipologie di comunicazione.

Alcune di queste metodologie sono i sistemi terminali (Dove si collegano tutti a un mainframe), l'architettura client/server e la peer-to-peer (che rimuove o limita l'utilizzo di server)

1.1 Collegamenti

Le reti di accesso si generalizzano in 3 categorie: accesso residenziale, accesso aziendale e accesso mobile.

L'accesso residenziale punto-punto utilizza tecnologie come la FTTH per fornire linee internet limitate a una residenziale. Le componenti tipiche sono il modem, il router, il firewall, il NAT e l'access point. Generamente ritroviamo tutte queste componenti unite nell'unico "router" casalingo

In un accesso aziendale le tecnologie aumentano, vediamo l'introduzione della LAN e collegamenti via Ethernet

Infine vediamo le tecnologie wireless, che, attraverso un access point, forniscono linea attraverso l'etere

Mezzi trasmissivi

Il mezzo fisico che connette i dispositivi rientra nella categoria dei mezzi guidati o nelle onde libere. Il mezzo guidato più comune è il filo di rame a doppino intrecciato (TP). Le sigle dei doppini identificano i vari tipi di schermatura, la parte sinistra è la schermatura dell'intero cavo (Unshielded, Foiled, Shielded o maglia metallica) e la parte destra indica il singolo doppino (Unshielded and Shielded). Questi casi possono anche essere più o meno incrociati (cross o patch) da un connettore all'altro. Questo permette di connettere direttamente due terminali.

Per I mezzi a onde libere abbiamo le microonde terrestri, le WiFi LAN, le Wide area e le satelittari. Questo tipo di propagazione è più vulnerabile agli effetti dell'ambiente di propagazione

Nucleo della rete

Il trasferimento dei dati nella rete avviene tramite commutazione di circuito o commutazione di pacchetto. Il primo metodo era quello classico della rete telefonica, il che comportava l'assenza di condivisione delle risorse. La rete viene suddivisa in porzioni con ripartizione della banda tramite divisione in frequenza o tempo. Nel caso le risorse non vengono utilizzate allora rimangono inattive

1.2 Struttura di internet

Internet è strutturato gerarchicamente. Nel punto più alto troviamo gli ISP di liv 1 che forniscono copertura nazionale se non addirittura internazionale. Le comunicazioni fra di loro vengono considerate fra pari (peer). Successivamente l'ISP di livello 1 vende copertura agli ISP di liv 2, che sono in

grado di comunicare con altri ISP di liv 2 e un numero limitato di ISP liv 1. Infine abbiamo infine le reti di ISP di liv 3 e reti locali. Queste reti vengono definite reti di ultimo salto (last hop)

In queste reti sono disponibili gli IXP (Internet eXchange Point), ovvero edifici dove gli ISP di livello 2 comunicano fra di loro direttamente

Ritardi e Perdite

Se troppi pacchetti arrivano in un router che non riesce a processarli in tempi brevi, allora i pacchetti vengono accodati. Questi problemi avvengono in 4 casistiche

elaborazione del nodo

Questi problemi avvengono a causa del controllo sugli errori del bit o per la scelta del canale d'uscita

Ritardo per accodamento

I pacchetti si fermano nel router in attesa di trasmissione o per congestione del router

Ritardo di trasmissione

Ritardo all'interno di un dispositivo di rete

Ritardo di propagazione

Ritardo dato dalla trasmissione del mezzo trasmissivo tra due dispositivi di rete

Quindi il ritardo del nodo è dato dalla somma di ritardo di elaborazione (processing delay), ritardo di accodamento (queuing delay), ritardo di trasmissione (transmission delay) e ritardo di propagazione (propagation delay)

$$d_{node} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

Un'altra formula importante è quella del ritaro d'accomodamento, che è dato dalla lunghezza del pacchetto per il tasso medio di arrivo dei pacchetti, il tutto fratto il bitrate

$$\frac{A \times L}{R}$$

1.3 Livelli di protocollo

Ogni protocollo viene organizzato su vari livelli in base al suo ruolo, questa strategia si chiama stratificazione e permette semplificare l'identificazione di un protocollo e le sue funzioni. Inoltre le modifiche a un determinato livello risulta trasparente rispetto agli altri layers.

I layer sono in grado di fornire servizi al layer superiore, mentre utilizzano quelle del livello inferiore. Questi servizi vengono forniti attraverso i SAP (Service Access Point). Questi layer sono 5 nella struttura Tcp/ISP

Applicazione

Fornisce alle applicazioni i mezzi per scambiarsi i dati. A questo livello le data unit si chiamano messaggi.

Transporto

Gestisce i problemi di qualità del livello di rete, applica la segmentazione e ricomposizione dei dati, multiplexing. Applica anche controlli di flusso, errore e riordino dei pacchetti. Le data unit vengono chiamate segmenti

Rete

Responsabile dell'instradamento dei dati tra un host e l'altro. Offre servizi connection-less o connection-oriented (l'indipendenza durante l'instadazione tra un pacchetto e l'altro). Le data unit vengono chiamate pacchetti o datagrammi

Collegamento

Si occupa di multiplexing, effettua controlli e correzzioni di errori e implementa il MAC (Medium Access Controll). Le data unit vengono chiamate frame

Fisico

trasferimento dei singoli bit sul mezzo di comunicazione (elettrico, elettromagnetico, luminoso,...). Fornisce i servizi per creare, mantenere e distruggere le connessioni fisiche

Nel modello ISO/OSI si aggiungono anche i livelli presentazione e sessione che si occupano di cifrature e sincronizzazione

1.3.1 Data units

In un sistema con N layers, i dati trasmessi compongono una N-SDU, o una Service Data Unit di layer N, dove viene poi incapsulata dalle Data Unit di livello inferiore formando una PDU (Protocoll DU).
Man mano che la PDU scende nei layer vengono aggiunti diversi header, che successivamente vengono disassemblate dal ricevitore. A causa delle dimensioni della PDU possiamo segmentarla in PDU di dimensione ridotta oppure unire diverse PDU di piccole dimensioni in un singolo messaggio

1.4 Sicurezza

Internet non è stato pensato con il pallino della sicurezza. Attraverso internet, gli attaccanti sono in grado di inviare virus, worms, e trojans, senza contare programmi di spionaggio e botnets. C'è anche la possibilità di anilisi dei pacchetti in transito sulla rete (packet sniffing), o l'invio di pacchetti con un indirizzo di origine falso (IP Spoofing) o il reinvio di pacchetti sensibili (Record-and-Playback)

2 Livello applicazione

2.1 Architetture delle applicazioni di rete

Architettura client server

I server sono host sempre attivi e con indirizzo fisso, mentre il client può disconnettersi, avere link dinamici e non comunicare direttamente con altri client.
Questa architettura ha la difficolta della scalabilità.

Peer-to-peer

Non viene usato un server sempre attivo, ma vengono usate coppie di host con la capacità di diventare inattivi o usare indirizzi dinamici. Questa architettura è facile da scalare ma difficile da gestire

Ibridi

Le versioni ibride sono molto differenti fra loro, ma prendendo in esempio skype, utilizza chiamate peer-to-peer, ma un server centralizzato per la ricerca degli indirizzi

Cloud

Un'insieme di tecnologie in grado di gestire dati con risorse distribuite in rete. Tutti i dati sono memorizzate in server farm

2.2 Processi comunicanti

all'interno dello stesso host, due processi comunicano utilizzando schemi interprocesso. I processi client e server esprimono processi che danno inizio alla comunicazione o attendono di essere contattato.

Socket

Un processo invia e riceve da una socket (o porta). Viene pressupposto che esista un'infrastruttura esterna in grado di trasportare il messaggio fino alla socket destinataria.

Per la communicazione oltre all'indirizzo IP viene anche esplicitata la porta sulla quale comunica in maniera da identificare il processo ricevente

2.3 Protocolli a livello applicazione

Esistono una marea di protocolli, ma principalmente si dividono in protocolli proprietari, come skype, o protocolli di dominio pubblico, come http,smtp,...

2.4 Interazione con il livello di trasporto

Il livello di applicazione usa diversi servizi dal livello inferiore, come la gestione della perdita di dati, il quantitativo di throughput, e servizi di sicurezza come la cifratura.

2.5 Protocolli

2.5.1 HTTP

Protocollo a modello client/server, dove il client esegue richieste di oggetti web e il server risponde con gli oggetti richiesti. HTTP usa una connessione TCP sulla porta 80. HTTP è un protocollo stateless, ovvero senza che il server tenga informazioni sulle richeiste del client.

Le connessioni HTTP sono sia persistenti che non, ossia possono inviare un singolo oggetto come molteplici. La comunicazione generalmente segue questa falsa riga:

1. il client inizializza una connessione TCP con il server
2. Il server accetta la connessione
3. Il client invia un richiesta con l'url della risorsa
4. Il server risponde inoltrando l'oggetto richiesto e chiude la connessione
5. il client riceve il file HTML e trova il riferimento agli oggetti richiesti

Il tempo di propagazione e ritorno tra due host viene chiamato Round Trip Time (RTT).

Le connessioni non persistenti richiedono 2RTT per oggetto, l'hoverhead del SO per ogni connessione e connessioni TCP parallele. Mentre nelle connessioni persiste il server lascia la porta aperta permettendo di spostare i messaggi all'interno della stessa connessione.

HTTP usa due messaggi: richiesta e risposta.
La richiesta è formata da una riga di richiesta (GET, POST, PUT, DELETE) e delle righe di intestazione e il corpo dell'entità.
La risposta è formata dalla riga di stato, righe di intestazione e dati.

Una pagina web è costituita da oggetti e un file base scritto in html. Ogni oggetto è referenziato da un URL (Uniform Resource Location)

HTTP utilizza i cookies per mantenere dati come autorizzazioni, stato delle sessioni, raccomandazioni. I cookie permettono ai siti di imparare molte cose sugli utenti.
Utilizzano quattro componenti: una riga nell'intestazione dei messaggi di richiesta e risposta, un file mantenuto sul sistema del client e un database sul sito

Un'altro servizio è quello della cache web, ossia un sistema che soddisfa la richiesta del client senza coinvolgere il server. Il client viene configurato per effettuare richieste a un proxy, nel momento in cui il proxy possiede già la risorsa richiesta, risponde direttamente al client, se no inoltra la richiesta al server d'origine.
Tutto questo processo permette di ridurre la latenza e il traffico internet

HTTP 2.0 è un'evoluzione focalizzata sulle prestazioni con l'obiettivo di utilizzare un'unica connessione dai browsers a un server.
Si basa su SPDY, un protocollo livello applicazione con l'obiettivo di trasmettere contenuti con la minima latenza tramite multiplexing, priorità delle richieste e compressione dell'header HTTP. Tutte le connessioni HTTP/2 sono persistenti

Il framing binario in HTTP 2.0 usa la stessa semantica ma una codifica diversa, con messaggi più piccoli e codificati in binario. Tutte le comunicazioni in una singola connessione TCP può portare molteplici stream di byte, ognuno con identificativo univoco. Ogni stream trasmette vari messaggi che sono composti a loro volta da frames, la più piccola unità di comunicazione. Questi frames possono essere interposti e riassemblati tramite il loro identificatore

Grazie al nuovo livello di framing binario, HTTP/2 consente l'uso del multiplexing, dove client e server possono dividere i messaggi in frame indipendenti, di intervallarli e ricomporli a destinazione. Con questo metodo l'ordine dei frames diventa critico per le prestazioni, infatti agli streams viene assegnato un peso da 1 a 256 con la quale l'host può definire degli alberi di priorità per l'invio dei frames

Ultima funzionalità è quella del server push, ossia che il server è in grado di inviare ulteriori risorse collegate a quella richiesta dal client con un'unica query. In questo modo le risorse necessarie per far funzionare un'applicazione web vengono inviate con un solo messaggio di risposta, risparmiando risorse e tempo al server

2.6 FTP

È un protocollo di tipo client/server che permette il trasferimento di file. Il servizio usufruisce della porta 21

2.7 Posta elettronica

Nella posta elettronica abbiamo 3 componenti principali: l'agente utente, il server di posta e il protocollo.

L'agente utente, o mail reader, si occupa di composizione, editing e lettura dei messaggi memorizzati sul server. Il server di posta contiene la coda dei messaggi, la casella di posta e gestisce il protocollo di comunicazione tra server e server per inviare e ricevere mails

2.7.1 SMTP

questo protocollo usa connessioni tcp persistenti per trasferire in modo affidabile le mail in maniera diretta. Il trasferimento è gestito in 3 fasi: handshake, trasferimento dei messaggi e chiusura. I comandi sono composti in un testo ascii 7 bit, e le risposte tramite codici di stato ed espressioni.
La porta usata è 465

Per l'utilizzo di messaggi multimediali, viene aggiunta l'estensione MIME

Protocolli d'accesso alla posta

Mentre SMTP gestisce il trasferimento tra un server e l'altro, POP,IMAP e HTTP vengono usati dall'agente utente per accedere al servizio di posta

2.7.2 POP3

POP è un protocollo senza stato che gestisce le autorizzazioni e i download. Esso offre varie modalità come scarica e cancella o scarica e mantieni per mantenere i messaggi su più client.
La porta è la 995

2.7.3 IMAP

IMAP è un protocollo più complesso di POP3, con più funzioni e la possibilità di manipolare messaggi sul server. IMAP tiene tutti i messaggi sul server, e permette all'utente di organizzarli in cartelle. IMAP inoltre mantiene lo stato dell'utente tra le varie sessioni.
La porta è la 993

2.7.4 TLS

È un protocollo crittografico sulla comunicazione che fornisce autenticazione, integrità e confidenzialità. Il processo è composto da una prima negoziazione sull'algoritmo da utilizzare, poi vieno lo scambio delle chiavi e l'autenticazione. Il resto della comunicazione avviene con una cifratura simmetrica e autenticazione dei messaggi.

La sua evoluzione è STARTTLS che cifra la connessione sulle porte originali. Viene usata soprattutto tra Mail Transfer Agents (MTAs) nel trasporto di una mail tra un provider e l'altro.

2.8 DNS

È un database distribuito che permette agli host di risolvere i nomi (o tradurre da nome a indirizzo). Questo struttura decentralizzata permette hal servizio di gestire un maggior volume del traffico e di essere più resistente a guasti.

La struttura gerarchica divide i server DNS authoritativi alla base per poi venire gestito dal DNS di dominio (.com,.org,...) o server TLD (Top-Level-Domain). Infine il punto più alto viene gestito da un server root del DNS.
Esistono anche i DNS locali. Non fanno propriamente parte della gerarchia, ma ogni società dispone di un default name server.

Quando i server root vengono contattati dai DNS locali, possono rispondere con la mappatura richiesta, ma se non possiede la mappatura, allora si occuperà di contattare il server autorizzato che possiede le informazioni richieste.
Una volta che un server impara una mappatura, essa viene tenuta in cache per un certo periodo di tempo.

I dati che vengono contenuti nel DNS vengono chiamati RR, o Resource Record, e contengono nome, valore, tipologia e TTL.

I messaggi DNS compongono query e risposte con lo stesso formato. L'itestazione contiene un valore d'identificazione della query, i flag (query, aswer, richieste di ricorsione...). Nei contenuti abbiamo la domanda, l'RR di risposta, il server di competenza e informazioni aggiuntive.

2.9 Condivisione P2P

Una distribuzione P2P è molto più efficente rispetto alla gestione del singolo server. Un modello molto usato è bitTorrent. Esso usa un server per tenere traccia dei peer che partecipano, e i torrent, o gruppi di peer che si scambiano parti di un file. Il file viene diviso in diversi chunk (generalmente 256kb) e distribuito a diversi peer vicini (o neighbors) durante il download.

La parte di corrispondenza tra le informazioni e la posizione di un host è una Hash table distribuita

In un servizio completamente distribuito viene definito query flooding, dato che senza un server centrale, rischia di riempire la rete. Infatti la query viene inoltrata sulla rete e rediretta ai peer vicini finche non viene trovato il destinatario

L'unione tra un indice centralizzato e query flooding è la copertura gerarchica, in questo caso ad alcuni peer viene assegnato il ruolo di leader di un gruppo e gestiscono le query per conto dei peer sottoposti.

2.10 Cloud computing

È un'architettura che prevede diversi server reali ad alta affidabilità e fisicamente locati in un data center del provider del servizio. In questo modo le caratteristiche fisiche sono irrilevanti per l'utente, a differenza di sicurezza, privacy e continuità di servizio

Content Delivery Networks

Una CDN costruisce una rete overlay per la distribuzione di contenuti, utilizzando il concetto chiave di disponibilità dei dati il più vicino possibile agli utenti. Questo metodo ottimizza le prestazioni di rete, riduce la latenza e evita i colli di bottiglia.
Sfrutta due metodi: Enter deep, dove gli ISP installano server in tutto il mondo, e Bring home, con meno server, ma installati negli IXP

DASH

Dynamic Adaptive Streaming over HTTP. È un servizio di streaming multimediale che divide i video in chunk e che permette al client di riceve chunk dello stesso video a server diversi, in modo da ottimizzare la visualizzazione e ridurre i ritardi

3 Livello di trasporto

I servizi e protocolli di trasporto forniscono la comunicazione tra host differenti. Dal lato invio il livello di trasporto scinde i messaggi in segmenti e lo passa al livello di rete,passando la comunicazione logica tra host, mentre dal lato di ricezione riassembla i messaggi e li passa al livello applicazione, passando la comunicazione logica tra processi.

3.1 Multiplexing e demultiplexing

Il multiplexing al trasmettitore gestisce i dati da diverse socket con l'aggiunta di un header PCI, mentre il demultiplexing usa le PCI per consegnare i segmenti alle socket giuste

3.2 TCP

È un protocollo affidabile, con consegne nell'ordine originario. Implementa controllo di congestione, flusso e setup della connessione.

NB: controllo di flusso opera sulla ricezione dell'host, mentre il controllo di congestione opera sulla m trasmissione in rete

3.3 UDP

Lo User Datagram Protocol è un protocollo best-effort, infatti i segmenti possono essere perduti o consegnati in ordine scorretto. UDP inoltre è un protocollo connection-less, quindi senza handshake e segmenti gestiti indipendentemente dagli altri

3.3.1 Checksum UDP

Per controllare che il segmento sia giunto senza errori viene fatta la somma delle parole e calcolato il complemento a 1 del risultato. questo valore viene poi inserito nel campo checksum del segmento UDP. Al ricevente basta poi rieffettuare la somma e sommare il checksum, se il risultato ha tutti i bit a 1, non è stato rilevato errore, se no il contrario.

3.4 trasferimento dati affidabile

3.4.1 ARQ

L'Automatic Repeat reQuest è una classe di protocolli con lo scopo di recuperare le perdite di pacchetti. Tra questi abbiamo:

- Stop&wait
- Go-back-N

- selective repeat
- TCP
- Protocollo MAC

Stop&wait

Il trasmettitore, dopo aver inviato il primo segmento, attende un ACK da parte del ricevente. Se non riceve l'ACK entro un timeout, allora reinvia la PDU. Il ricevitore può scegliere di non inviare l'ACK in caso la PDU risulti errata o in disordine.

Pipelining

Questo metodo afferma che il trasmettitore consideri l'esistenza di ACK "in volo", cioé inviati ma non ancora ricevuti. Il selective repeat e go-back-N usano questa tecnologia.

Alcuni termini utili sono:

- finestra di trasmissione: l'insieme di PDU che vengono inviate dal trasmettitore senza aver ricevuto l'ACK
- Finestra di ricezione: insieme di PDU che il ricevitore può accettare e immagazzinare
- puntatore low: puntatore al primo pacchetto della finestra di trasmissione
- puntatore up: puntatore all'ultimo pacchetto già trasmesso

Gli ACK utilizzati possono essere di diverso tipo: ACK individuale, ACK cumulativo (ho ricevuto fino a n), ACK negativo (NACK) e piggybacking (ACK inseriti dentro altre PDU)

Go-back-N e selective repeat

Il Go-back-N invia cumuli da N pacchetti, e il ricevente invia solo ACK cumulativi. Il timeout è impostato sulla base del pacchetto più vecchio. Nel selective repeat invece il ricevente invia ACK dei singoli pacchetti. Con questo metodo il mittente deve tenere un timer per ogni pacchetto

3.5 TCP

Parliamo di un protocollo point-to-point, full-duplex, orientato alla connessione che implementa pipelining e un flusso controllato e affidabile.

La struttura contiene campi come l'ACK, checksum, finestra di ricezione (RWND), lunghezza massima del segmento (MSS), retransmission timeOut (RTO) e flag di controllo della connessione.

Il setup della connessione avviene seguendo specifici passaggi:

1. Host A invia un segmento con flag SYN=1, nel pacchetto è contenuto porta sorgente, destinazione e numero di sequenza iniziale
2. Host B invia un ACK con flag SYN=1 e ACK=1, nel pacchetto contiene in valori precedenti più il numero di ACK
3. Host A risponde con un segmento con flag ACK=1, il pacchetto non contiene numero di sequenza

La chiusura della connessione invece è bidirezionale e usufruisce del flag FIN=1 con relativo ACK da entrambi gli host. Esiste anche la chiusura tear down, più brusca, che usa il flag RST=1 per resettare la connessione

3.5.1 Controllo di flusso

Questo meccanismo permette al ricevitore di controllare la velocità di trasmissione del mittente.

Nel caso TCP, il ricevitore comunica le dimensioni della propria finestra di ricezione tramite il campo RWND. Il mittente, ricevuti i dati, si riadegua per non mandare in overflow in buffer del ricevente.

3.6 Principi del controllo di congestione

Con congestione intendiamo il fenomeno in cui la rete riceve più pacchetti di quelli che riesce a gestire. Questo comporta la perdita di pacchetti e ritardi.

Un modello a code comprende un lista d'attesa per un server. Il tasso di frequenza d'arrivo è il numero medio di pacchetti in arrivo in un lasso di tempo, mentre il tasso di frequenza di servizio è quanto velocemente vengono processati

3.6.1 Cause e costi della congestione

una congestione può rientrare in 3 categorie:

- Buffer infiniti

  nessuna perdita, ma più il tasso di arrivo si avvicina a quello di servizio più aumentano i ritardi

  costo: ritardi molto elevati

- Ritardi dovuti lla congestione: timeout

  costo: spreco di risorse dato da ritrasmissioni inutili

- pacchetti scartati a causa della congestione

  costo: ritrasmissioni, questo porterebbe a un maggior lavoro per ottenere lo stesso thorughput percepito a livello applicazione

3.7 Controllo della congestione in TCP

Esistono diversi tipi di approcci alla congestione in TCP:

- controllo di congestione end-to-end
- controllo di congestione assistito dalla rete

Gli algoritmi utilizzati da TCP sono:

- In assenza di perdite:
  Slow start
  Congestion avoidance
- In caso di perdite:
  Fast retransmit
  Fast recovery

3.7.1 AIMD

L'Additive Increase Multiplicative Decrease è un approccio in cui il mittente aumenta il tasso di trasmissione cercando di occupare più banda possibile, finche non si rilevano perdite. Praticamente si aumenta la finestra di 1 MSS ogni RTT finché non ci sono perdite, e successivamente si riduce la finestra della metà. Questo metodo garantisce più equità fra le sessioni

3.7.2 Slow start e Congestion avoidance

Nello Slow start, per ogni ACK ricevuto, aumento la finestra di congestione di 1 MSS. Nel momento in cui supero la soglia di congestione, entro in modalità congestion avoidance. In questa modalità, per ogni RTT in cui ricevo tutti gli ACK attesi, aumento la finestra di congestione di 1 MSS

3.7.3 Fast retransmit e fast recovery

Alla ricezione del terzo ACK duplicato ritrasmetto il segmento indicato dall'ACK ed entro nella fase di fast recovery. Abbasso la soglia dello slow start e ricomincio a salire in maniera adittiva fino all'arrivo di un ACK valido. A quel punto passa in congestion avoidance

NB: throughput tcp: $< \frac{MSS}{RTT} \cdot \frac{1}{\sqrt{p}}$

3.7.4 Controllo di congestione - CUBIC

CUBIC fa variare la lunghezza della finestra di congestione secondo una funzione cubica del tempo. Per compabilità con TCP, CUBIC si comporta come TCP standard in una rete con RTT brevi

3.7.5 BBR

Bottleneck Bandwidth and ROundtrip propagation time è un algoritmo che si basa sull'RTT e la banda sul bottleneck.
È un protocollo progettato per rispondere a una congestione effettiva piuttosto che alla perdita di pacchetti, ed è implementato solo sui server (Server-side algorithm).

Oltre che ad evitare congestioni, BBR presenta anche riduzioni significative della latenza

3.7.6 QUIC

QUIC mira ad essere equivalente a tcp ma con una latenza inferiore. Basato su UDP con un overhead ridotto, sfrutta l'handshake iniziale di TLS per inviare anche i dati necessari per i pacchetti futuri.

Ogni flusso è controllato separatamente, in maniera che lo stack di protocollo non è fermato da un singolo flusso.
Inoltre, QUIC usa degli identificatori di connessione, che risultano indipendenti al cambio di rete, al contrario di TCP che si rallenta per ripristinare le connessioni

4 Livello di rete

4.1 Visione d'insieme

Le due operazioni principali a livello di rete sono il forwarding e il routing. La prima è un'operazione con scala locale che sposta un pacchetto dall'entrata all'uscita di un router, mentre la seconda è a scala globale e determina il percorso che il pacchetto deve seguire. Le due parti si suddividono nel data plane e control plane, le logiche locali e globali del router

4.2 Il router

possiamo dividere il router in processore (software, control plane) e porte d'ingresso, uscita e sistema di commutazione ad alta velocità (hardware, data plane)

4.2.1 Porte d'ingresso

Composte da terminazione di linea, protocollo di ricezione e buffer, utilizzano gli header per indirizzare i pacchetti alla porta d'uscita corretta tramite le tabelle di inoltro, cercando di non introdurre ritardi ulteriori

4.2.2 Sistemi di commutazione

Usano tre strutture: a memoria, a bus e a matrice. La commutazione a memoria è la più vecchia e utilizzava la CPU per l'indirizzamento. La commutazione a bus usa un bus dati condiviso per trasmettere il datagrammi alle uscite. Infine la commutazione a matrice usufruisce di punti di intercocnnessione tra line d'ingresso ed uscita

4.2.3 Porte d'ingresso ed uscita

un commutatore più lento delle porte causa accodamenti agli ingressi. Quando un datagramma al primo posto della coda blocca quelli successivi è chiamato Head of line (HOL). Alle porte d'uscità invece vengono applicate delle politiche di scheduling. La dimensione dei buffer è definita nella RFC 3439, ossia un RTT generico moltiplicato per la velocità del link, il tutto diviso dalla radice del numero di flussi disponibili

4.2.4 meccanismi di scheduling

Lo scheduling avviene per meccanismo FIFO, ma nel momento in cui la coda si riempie, vengono usati 3 metodi per lo scarto dei pacchetti: tail drop (scarto pacchetti in arrivo), priority drop e random drop

4.3 Protocollo IP

4.3.1 Datagramma

I campi del pacchetto ip sono: VER (versione), lunghezza header, tipo di servizio, lunghezza totale, id, flag, offset, TTL, protocollo superiore, checksum, ip sorgente, ip destinazione, opzioni ip, padding

4.3.2 frammentazione

Ciascuna rete diversa può richiedere una MTU, o limite dati massimo di trasmissione, specifica, perciò il router frammenta i datagrammi e li invia impostando il flag che indica la frammentazione e il campo offset specificando come concaternare i frammenti. Inoltre copia i campi necessari dall'header originale.
I flag che vengono usati sono D (do not fragment) e M (more fragments comming)

La frammentazione a livello IP è disabilitata su internet per mitigare gli attacchi di overlapping fragments, DDos di riempimento di memoria e errori di assemblaggio dei frammenti

4.3.3 indirizzi IP

gli host e router devono usare le stesse convenzioni, l'indirizzo IP pubblico deve essere unico, ogni interfaccia ha un indirizzo IP

Gli indirizzi IP sono generalmente divisi in due parti:

- Prefisso: l'identificatore della rete (NetID)
- suffisso: identifica l'interfaccia di rete (HostID)

in passato venivano usate diverse classi di indirizzi, con diverse lunghezze dei prefissi

Le autorità per l'assegnazione degli indirizzi sono l'ICANN (Internet Corporation for Assigned Names and Numbers) che usano i registrar per consentire agli ISP di gestire blocchi di indirizzi

4.3.4 Indirizzamento classless

Il metodo classless permette agli ISP di assegnare prefissi di rete che permettono di gestire numeri specifici di host. Quindi per determinare la dimensione del prefisso si utilizzano le maschere di rete, ossia 32 bit impostati a 1 fino al prefisso. Questo metodo permette un uso efficente dell'AND logico per determinare il NetID.
La notazione /x è chiamata notazione CIDR

L'inoltro con CIDR usufruisce della subnet per determinare la rete e l'interfaccia ad essa collegata. In caso di multiple corrispondenze si usufruisce della regola del longest prefix matching

I router usufruiscono di una tabella di routing per definire ad ogni interfaccia quali reti sono collegate

4.3.5 Indirizzi pubblici e privati

La maggioranza di indirizzi IP è pubblica e vengono gestiti dagli ISP, mentre invece per le reti a gestione privata vengono riservati 3 intervalli di indirizzi:

- 10.0.0.0/8 (fino a 10.255.255.255)
- 172.16.0.0/12 (fino a 172.31.255.255)
- 192.168.0.0/16 (fino a 192.168.255.255)

4.3.6 Indirizzi speciali

Ecco un elenco di indirizzi speciali in IPv4:

- Indirizzi di rete

  Usati come riferimento ad una rete, impostano tutti i bit HostID a 0

- Indirizzi broadcast di una rete

  Sono indirizzi broadcast che possono essere inoltrati da un router a una determinata rete. Si ottengono settando tutti i bit HostID a 1

- Indirizzo broadcast di una rete locale

  255.255.255.255: Usato per la comunicazione broadcast locale, non viene inoltrato dai router

- Indirizzo sconosciuto

  0.0.0.0: Usato per determinare indirizzi non validi o non ancora assegnati, come all'inizio di un discovery DHCP

- Indirizzo di loopback

  127.0.0.1: Usato da un host per comunicare con se stesso. Per esempio viene usato per testare le app di rete

- Indirizzi multicast

  Usati per inviare pacchetti a un gruppo di host, iniziano tutti con 1110 (224.0.0.0→ 239.255.255.255). Il traffico multicast è minimo, molto spesso bloccato su internet

- Indirizzi link-local

  169.254.0.0/16: una sottorete usata per le comunicazioni quando un host non riesce a trovare un indirizzo IP

- Indirizzi per router

4.3.7 Network Address Translation

Per connettere reti con indirizzo privato a internet, vengono usate due tecnologie: un proxy (dispositivo con un indirizzo pubblico e uno privatio che fa da middleman) e il NAT, ossia un apparato che si interfaccia a internet e effettua una mappatura degli indirizzi privati convertiti in porte dell'indirizzo pubblico.
NAT offre 60 mila connessioni simultanee grazie alle porte a 16 bit.

4.3.8 ARP

L'Address Resolution Protocol viene utilizzato per trovare l'indirizzo MAC asseggnato ad un determinato indirizzo IP. Il funzionamento si basa su una richiesta in broadcast fatta dal mittente alla ricerca di un destinatario specifico. Se un host corrisponde a quel destinatario risponde con il suo indirizzo MAC, se no scarta il messaggio.

Per evitare di floodare la rete con richieste ARP, le risposte vengono salvate in memoria, e in caso di nuove corrispondenze, le vecchie risposte vengono sovrascritte o scartate dopo 30 secondi

Una macchina può anche essere configurata come ProxyARP, ossia una macchina che inoltra i messaggi ARP su un'altra rete spacciandosi come host mittente. Questo sistema permette di gestire sottoreti come una rete unica

4.3.9 ICMP

Questo è un protocollo usato per la gestione e manutenzione delle reti. Funziona in simbiosi con IP dato che IP usa ICMP per segnalare gli errori, e ICMP usa IP per trasportare i messaggi. Questi messaggi sono molteplici, ognuno con il proprio ruolo. Alcuni esempi sono destination unreachable, time exceeded, redirect...

5 Data link

Gli host e i router si comportano come nodi di una rete, mentre gli archi sono i vari link, che possono essere sia cablati che wireless.
I pacchetti di livello data link sono chiamati frame.

Il compito di questo livello è il trasporto da un nodo all'altro, nonostante i link possono essere di vari tipi e con protocolli (con i relativi servizi) diversi.
Nello specifico, la creazione di un frame avviene tramite:

- Incapsulamento di un datagramma in frame, con relativi header e trailer
- Fornitura di un meccanismo d'accesso al canale di comunicazione
- Identificazione di mittente e destinatario tramire indirizzo MAC

Viene anche implementato un controllo di errore per le connessioni con alti tassi d'errore.
Altri servizi offerti dal livello datalink sono il controllo di flusso, correzzione d'errore e comunicazione half/full-duplex

Il livello datalink viene implementato dall'adattatore di rete all'interno di un host

5.1 Rilevamento di errori

Nel datagramma, oltre che il controllo di parità, esiste il campo EDC (Error Detection and Correction) che contiene il numero di bit ridondanti inseriti.

Viene usato CRC (Cyclic Redundancy Check), ossia l'algoritmo più efficente per il rilevamento di errore

5.2 Tipi di collegamento

Nel momento in cui due o più trasmissioni partono simultaneamente da nodi diversi si può generare un'interferenza. Per questa ragione è necessario un protocollo di accesso multiplo ad un mezzo. Questi protocolli si chiamano MAC (Multiple Access Control) e rientrano in tre tipi di classi:

- Ripartizione delle risorse del canale (cioé creando sotto canali)
- ad accesso casuale
- A turni intelligenti

5.3 CSMA

il Carrier Sense Multiple Access è un tipo di approccio a un canale dove si "ascolta" prima di iniziare la trasmissione

Si definisce come CSMA 0-persistente (non persistente) quando un nodo, cercando di trasmettere su un canale occupato, attende un quantitativo di tempo casuale prima di ritentare la trasmissione. Un'altra versione è CSMA 1-persistente, dove il nodo attende finché il canale non è libero per poter trasmettere. In caso di collisione, il nodo attente un tempo casuale prima di ripetere la procedura