

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 satellitari. 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 ritardo d'accodamento, 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 correzioni 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 analisi 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 difficoltà 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 presupposto che esista un'infrastruttura esterna in grado di trasportare il messaggio fino alla socket destinataria.

Per la comunicazione 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 richieste 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 una 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'overhead del SO per ogni connessione e connessioni TCP parallele. Mentre nelle connessioni persistenti 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 viene 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). Questa struttura decentralizzata permette al servizio di gestire un maggior volume del traffico e di essere più resistente a guasti.

La struttura gerarchica divide i server DNS autoritativi 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'istanza contiene un valore d'identificazione della query, i flag (query, answer, 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 efficiente 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 finché 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 ricevere 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 trasmissione in rete

3.3 UDP

È un protocollo best-effort, con consegne senza ordine