DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

CoScienze
Associazione

NOZIONI GENERALI: RIPETIZIONE DEI CONCETTI BASE DI RC.

Rete di calcolatori: Un insieme di dispositivi (nodi) indipendenti, interconnessi tra loro tramite un canale di comunicazione.
Vantaggi: Condivisione delle risorse, collaborazione
Svantaggi: Gestione complessa

Struttura di internet: Suddivisa in 3 layer, in ognuno di essi sono presenti degli ISP (internet service provider). Al 1 livello ci sono gli ISP internazionali, connessi tra loro. Al livello 2 troviamo gli ISP regionali, connessi ad alcuni ISP di 1 livello (pagando) e 2 livello (si dicono pari di grado "peer"). Al livello 3 gli ISP locali, clienti degli ISP di livello 2.

Protocollo di rete: definisce il formato e l'ordine dei messaggi scambiati tra due o più nodi. Gli elementi chiave di un protocollo sono la sintassi (formato), la semantica (significato), sincronizzazione dei messaggi. Diversi protocolli vengono utilizzati nell'application e transport layer ma a livello network viene utilizzato solotanto il protocollo IP.

Standard: forniscono linee guida a chi sviluppa una rete pubblica. Divisi in due categorie: "de facto" non ufficiali ma utilizzati, "de jure" riconosciuti ufficialmente.

HTTP è un protocollo utilizzato nel web per trasmettere diversi tipi di informazioni. La sua sintassi è basata su MIME.
Una *richiesta* http è formata dai campi: Request line (contenente diversi campi di informazione), header lines (più linee contenenti informazioni sugli header quali: nome dell'header, valore ecc.), Body del messaggio (opzionale).
La *risposta* è indicata con un codice che ne caratterizza la tipologia.
Problema: http usa solo TCP come protocollo di trasporto, non ottimizzato per connessioni frequenti e di breve durata.
Possibile soluzione 1: invio di più richieste e risposte in una connessione TCP. Vantaggi: ottimizzazione, Svantaggi: non si sa quando chiudere le connessioni.
Soluzione 2 (pipelining): Trasmissione seriale di richieste senza attendere risposta, queste ultime dovranno essere restituite nello stesso ordine. Vantaggi: ulteriore ottimizzazione.

Proxy (edge server): Localizzati al centro della comunicazione tra user agent e origin server per ridurre il carico di questi ultimi. Agisce come server per il client e come client per il server.

Gateway: Agisce da intermediario per i server non http, il client comunica in http con il gateway e quest'ultimo in un altro linguaggio con il server. Motivi di utilizzo:

- Condivisione di accesso al web per ottimizzare l'utilizzo della rete.
- Caching: vengono mantenute copie in locale dei documenti più popolari così da non doverli ritrasmettere.
- filtering: alcune pagine possono essere filtrate eliminando alcuni contenuti
- Accesso controllato a documenti: per documenti sensibili può essere implementato un proxy che si accerti dell'identità del richiedente.
- Reverse proxies: Proxies che si mascherano da web server per migliorare le performance di un web server.
- Router di contenuti: utilizzati per formare una rete di contenuti replicati

- Traduzione dei contenuti: il proxy può tradurre la lingua di una pagina o modificarne i contenuti in base al device che accede al servizio
- Rendere anonimo: il proxy può rendere anonimo il client eliminando le informazioni identificative dai pacchetti http.
- Protezione della privacy durante la navigazione web
- Blocco delle richieste di informazioni verso siti di terze parti. Effettuato tramite alcune tecniche quali: eliminazione cookie di terze parti, bloccare l'esecuzione di codice dinamico nelle pagine, bloccare banner e richieste per siti di terze parti

Tunnel: tecnica utilizzata per veicolare informazioni che utilizzano altri protocolli attraverso l'http. Cambia dunque la sintassi (formato) dei dati.

Web Server (http server): risponde alle richieste di risorse effettuate dal client. Le fasi per la gestione della richiesta sono:

- Parsing della richiesta: lettura delle informazioni nella richiesta
- Check di autorizzazioni: controllo dei permessi di accesso alla risorsa tramite una access control list
- Associazione URL con filename: a partire dall'URL viene trovato il filesystem
- Costruzione della risposta: può essere generata in modo dinamico tramite script o in modo statico prelevando la risorsa richiesta
- Trasmissione della risposta

Mantenimento dello stato in un protocollo stateless tramite i cookie scambiati tra request e response
Il caching è una pratica per ottimizzare la fornitura di file richiesti di frequente mantenendoli in memoria.

Architettura Web server:
Single-Threaded, serve una richiesta per volta, scarse prestazioni.
Multi threaded, utilizzati più thread per soddisfare più richieste in contemporanea, il numero di thread ha un tetto massimo per non saturare le risorse.
Multiplexed I/O: utilizzata per un elevato numero di connessioni per ogni thread.
Multiplexed multithread: Combinazione di multithreading e multiplexing.

Benchmarking: Processo continuo di misurazione di prodotti mediante il confronto con i concorrenti più forti del settore. Utilizzato per incrementare le performance del prodotto.

Esistono diverse tipologie di benchmarking, per ogni settore economco.
Web Server Benchmarking: effettuati per verificare la capacità di carico del server.
Parametri di misurazione:

- Numero di richieste servite al secondo
- Tempo di risposta per ogni nuova connessione
- Throughput (bytes/sec)

Procedura di benchmarking: usare la stessa configurazione per tutti i test, eseguire il test, eseguire il reboot del server dopo ogni test.

Apache performance tuning:

l'architettura modulare di apache permette di caricare solo i moduli necessari, il modulo "mod_so" deve essere compilato staticamente per abilitare i DSO (Dynamic shared objects).
La compilazione statica dei moduli permette di risparmiare la RAM. Altri moduli possono essere aggiunti con la direttiva LoadModule.
La scelta dell'MPM dipende da diversi fattori:

- MPM Worker: Pochi figli, ognuno gestisce più connessioni,
  Vantaggi: veloce, scalabile, poca memoria. Svantaggi: thread non corretti influiscono sugli altri child process.
- MPM Prefork: Molti figli, ognuno gestisce una connessione, Vantaggi: velocità simile al worker, Svantaggi: molto uso della memoria.

Dns lookup: abilitato con la direttiva HostnameLookups, disabilitato di default, permette di loggare hostname e non indirizzo IP. Per le direttive Allow from e Deny from bisogna usare IP e non hostname.

Max Clients: fissa il numero massimo di client che possono accedere in contemporanea nel server, per evitare sovraccarichi. Valore appropriato = RAM del web server/Numero massimo di processi figli.

MaxSpareServers e MinSpareServers: determinano quanti processi figli mantenere in attesa di soddisfare le richieste. Un buon valore è un valore tale da non far generare più di 4 processi figli al secondo ad apache.

StartServers: definisce il numero di child creati allo startup.

MaxRequestPerChild: definisce il numero limite delle richieste che un server potrà gestire per ogni figlio. Il processo figlio termina dopo aver gestito quel numero di richieste. Di default il valore è 0 e il processo non termina mai.

È possibile utilizzare due server separati per la parte statica e dinamica per risparmiare memoria. È possibile usare un tiny apache come front end statico. Le richieste per i contenuti dinamici possono essere rimandate ad un'altra versione di apache. Il **request forwarding** viene eseguito con i moduli "mod_proxy" e "rewrite_module".

httpRef: tool di benchmark per misurare web server e proxy performance. Permette di misurare il numero massimo di richieste al secondo che il web server può sostenere, il tempo impiegato per rispondere alle richieste. Formato da tre componenti:

1. Core http engine: si occupa delle connessioni, delle richieste e delle risposte
2. Workload generator: genera stream di richieste http.
   a. Default: genera un numero fissato di http get misurando il numero di risposte

   b. --wlog=B,F : itera le richiesta su una lista di URI. F rappresenta il path al file che contiene la lista. Se B=n allora httpref si ferma alla fine della lista. Se B=y httpref ritorna all'inizio della lista.
   c. --wsess=N1,N2,X : Misura ressioni e non singole richieste. N1 rappresenta il numero di sessioni da generare, N2 il numero di chiamate per sessione, X lo user think time.
   d. --wsesslog=N,X,F: N è il numero di sessioni da generare, X il burst to burst (burst= numero fissato di chiamate al server) user think time, F il file.
   e. –wset=N,X : Itera attraverso una lista di Uri ad un dato rate. N è il numero di URL, X rappresenta il rate a cui si accede alle URL.
3. Statistics collector: misura vari parametri e produce un report con statistiche.

Internet measurement and architecture (CAP 2)

Internet: interconnessione di reti (o collezione di reti) appartenenti a diversi proprietari, infatti non esiste una singola autorità che lo gestisce.
E' importante sapere che Internet non può essere misurato, ovvero non si può stimare un consumo "globale" dell' utilizzo della rete, non esistono quindi misure quantitative.Le motivazioni sono le seguenti:

- Struttura decentralizzata: internet è costituito da varie organizzazioni .
- Natura dinamica: cambia continuamente in taglia, traffico, configurazioni , ecc.
- Altri fattori tecnici: Proprietà nascoste dall' architettura di internet che interferisce(reti nascoste) , dati difficili da memorizzare, trasferire ecc.. , inoltre il fattore privacy non ci permette di ottenere alcune forme di measurement .

Misurare è importante, tuttavia però ci sono varie problematiche. Le ragioni del measurement riguarda fattori principalmente commerciali , sociali e tecnici:

- Commerciali: Per vendere un prodotto, mi interessa sapere l'area adeguata dove il prodotto può "funzionare".
- Sociali: Un nuovo servizio deve attrarre una determinata platea di utenti, bisogna quindi capire se effettivamente può esserci il giusto interesse.
- Tecnici: Problematiche maggiormente prese in considerazioni. I progetti di componenti e protocolli sono guidati dalla natura dei workloads Inernet. Il traffico di internet porta perciò a rivedere le caratteristiche dei router che devono gestire il traffico internet.Un altro caso sono le pagine Web, infatti con il passare degli anni, esse richiedono performance maggiori.

In generale quindi è necessario capire le caratteristiche del traffico di reti esistenti , cosi da sviluppare modelli di traffico per reti future: la rete si espande e bisogna garantire comunque valide risposte in termini di performance.
L'architettura di internet è partita da 4 nodi ARPANET, ed era basata sul packet switching (dati trasmessi in pacchetti).
I nodi man mano aumentarono e si arrivò all' introduzione del TCP/IP che portò alla crescita della rete Internet. In seguito ad una riorganizzazione interna di ARPANET, i servizi offerti dalla rete sono implementati usando routers interconnessi tramite links gestiti da differenti organizzazioni. I router comunicavano con altri router sulla rete, e pertanto l'aumento del traffico portò all' introduzione degli **autonomous system (AS)**, insieme di router e link sotto un'unica amministrazione (ISP).
Un **Backbone** è un punto centrale della rete che interconnette quest'ultima con altre reti. Internet non ha un backbone singolo ma diversi ISP che eseguono diversi backbone tra loro.
L'**architettura di internet** è un'architettura circolare a tre livelli dal centro verso l'esterno (ISP di 3 livelli).
ISP di 1 livello: Nazionali e internazionali (es.Telecom) forniscono l'accesso al traffico verso la rete esterne, sulle grandi distanze.
ISP di 2 livello: soprattutto copertura nazionale , si connettono solo ad alcuni ISP di 1 livello per instradare il traffico verso altre reti.

ISP di 3 livello: Dove si collegano di utenti.

Gli AS scambiano traffico in punti di connessioni detti **peering points** attraverso i gateway routers.
Stateless switching: i pacchetti vengono instradati,i router non mantengono alcuna informazione sulle connessioni che li attraversano.

Componenti di internet:

- Endsystem: sono sistemi trasmittenti e riceventi e possono essere client, server o peers
- Router: utilizzati per instradare i pacchetti nella rete. Utilizzano una coda FIFO per gestirli, se si riempie vengono scartati.
- Links: connessioni sulle quali viaggiano i pacchetti. Ha a che fare con ritardo di propagazione e capacità.
- Wireless: dispositivi senza fili che permettono la connessione alla rete.

Routing: i pacchetti si muovono da un router all'altro nella rete senza un percorso preciso, ma deciso a momento. Il routing di internet è gerarchico ed avviene sia interno agli AS (inter domain routing) che tra gli AS (inter domain routing). All'interno di un AS tutti i router usano lo stesso protocollo, all'esterno si possono usare diversi protocolli, questo è un vantaggio che ha portato all'uso del routing gerarchico.

Open Shortest Path first: utilizzato per il routing all'interno degli AS. Tutti i router mantengono una mappa della rete dell'AS per calcolare il miglior percorso, la mappa viene sempre aggiornata. Se avviene un cambiamento un router avvisa tutti gli altri.

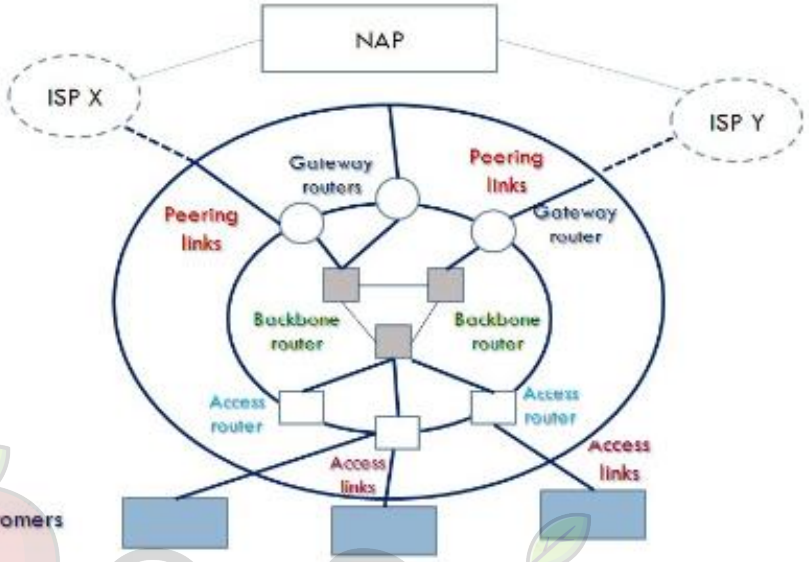
Protocollo BGP (Border gateway routing): utilizzato per il routing tra gli AS degli ISP. Permette di specificare delle politiche di instradamento per scegliere il cammino migliore. Viene realizzato tramite lo scambio di messaggi BGP contenenti dei path vector

Protocollo ICMP: utilizzato per il network monitoring e management. Prevede dei messaggi per la richiesta di informazioni ai router e il report di errori nel processo dei pacchetti. Ping e traceroute sono implementati con questo protocollo.

CAPITOLO 4: Pratical issues

4.1 Dove vengono fatte le misurazioni:

Le misure di internet possono essere effettuate in qualunque punto della rete con hardware o comunque con software sofisticato:
- vicino ai routers. – su link che connettono i routers. – su LAN. – sugli entry point della rete. – all' intetno di network backbones. – sulla rete geografica (WAN).



In questo schema vediamo:

- Backbone, access (tra ISP e customer tramite links) e gateway (tra diversi ISP, detti peering) sono router che comunicano tra loro.
  I gateway routers comunicano utilizzando il protocollo BGP, per lo scambio del traffico verso l'esterno della rete.
- NAP (Network Access Point) Rappresenta il punto di scambio di multipli internet service provider.

I test sulle LAN non hanno interessi significativi, restituiscono misurazioni più precise. Di norma si misura nei backbones per rilevare attacchi, cambio topologia , effettuare capacity planning, ecc.

Tecniche di raccolta dati per capacity planning:

- Meccanismo di polling di SNMAP per raccogliere caratteristiche del traffico
- Packet tracing dei pacchetti sul backbone

Allocazione di banda: attività effettuata dagli ISP per ridurre la latenza su determinate applicazioni

Le misurazioni nei backbone(per garantire capacity planning) forniscono una vista precisa di tutto il traffico associato ad un insieme di customers, utili per fornire servizi personalizzati e verificare i SLA. Queste misurazioni permettono di monitorare la rete per

attacchi. Per verificare se sono necessari ulteriori Point of services, utilizzo due tecniche:
1. Mediante SNMP , un protocollo con agent messi su componenti di rete che forniscono varie informazioni sui dati (packet loss, delay, througput)
2. Fare Packet tracing: Tecnica che fornisce piccoli timescale (sotto il secondo) di traffico, per identificare burst di traffico, se essi si verificano significa che bisogna aumentare la capacità, per mantenere alte prestazioni.

Misurazioni sugli Entry points della rete: Per filtrare contenuti non voluti. Per fare analisi del traffico si usano sitemi che analizzano flussi di traffico, nello specifico questa cosa è permessa da un tool, chiamato NETFLOW. Si possono ottenere varie informazioni come ad esempio il traffico che è destinato ai Customer.

Misurazioni nei peering routers: misurazioni effettuate per assicurare che i volumi del traffico siano bilanciati. Gli AS possono essere anche privati e lo scambio di dati tra due AS di questo tipo è noto solo ad essi. Sono utili per verificare che il traffico è bilanciato , secondo quanto stabilito nel SLA.

Misurazioni negli access routers: atte a verificare i SLA poiché si collegano al customer.

Misurazione in WAN: effettuate per misurare in modo simultaneo la rete da locazioni multiple distanti. Richiede la sincronizzazione dei clock. Essenzialmente i problemi legati al tempo sono associati a questo tipo di test.

4.2. Ruolo del tempo nelle misurazioni: 27:23

Le informazioni sul tempo sono requisiti importanti sulle misurazioni di internet, siccome quest'ultimo è distribuito. Le componenti possono trovarsi su grandi distanze, ciò genera il problema del clock globale, come anche ritardi di latenza ed altri fattori, per questo il tempo risulta essere fondamentale.Il tempo si può acquisire in vari modi, ad esempio si possono usare sorgenti esterne(radioclock (precisione estrema, millisecondi)) si possono inoltre utilizzare anche clock software e clock hardware.
Per introdurre tempi sincronizzati si usa il protocollo "Network time". Si basa sul fatto che si rilevano i tempi di latenza dei pacchetti in transito sulla rete.

Nozioni:
- offset: differenza fra il tempo riportato dal clock al tempo t e il true time.
- Skew: differenza tra il rate e il rate corretto.

Il tempo è importante anche per misurare il packet delay, ovvero quanto tempo impiega il pacchetto per effettuare tutto il percorso. Per fare ciò mittente e destinatario devono avere i clock sincronizzati.

Network time protocol: permette la sincronizzazione dei clocks in una rete a pacchetti, utilizzato universalmente a questo scopo. Formato in insieme gerarchico di client e server, un server si sincronizza confrontando il clock con quello di server allo strato superiore o dello stesso strato.

In generale lo strato 1 è sincronizzato con la fonte esterna (es. orologio atomico, gps, ecc.), lo strato 2 riceverà i dati dallo strato 1 e da tutti i server sul suo strato.
Lo strato 3 allo stesso modo riceve informazioni dallo strato 2 e dai server dello stesso stato tre. Si cerca quindi di aumentare al max la precisione eliminando i server scorretti. Si sincronizzano i clock, arrivando ad un valore che sia quanto più preciso.

Funzionamento: il client invia un messaggio NTP al server contenente il timestamp (marca l'invio) all'invio, il server inserisce il timestamp alla ricezione e riinvia in messaggio al client aggiungendo il timestamp dell'invio. Il client riceve il pacchetto e aggiunge il timestamp della ricezione e analizza i 4 timestamp. Da questi 4 , si ottiene il delay e l'offset, che servono per determinare il clock.

Un altro particolare caso riguarda i Database:
Per le misurazioni che comprendono l'accesso a database possono sorgere problematiche legate ad autorizzazioni o dati vecchi.

Misurazioni attraverso diversi protocolli di rete:
Il meccanismo di data gathering cambia a seconda del layer del protocollo, 3 categorie:

- Lower level protocol data (router e link, livello più basso): troppi dati da esaminare, e da processare velocemente: Una possibile tecnica consiste nel pooling e nella raccolta periodica dei dati. E' possibile risolvere raggruppando insiemi di comunicazioni in flussi e pubblicando periodicamente un record contenete le informazioni chiave sul traffico scambiato (indirizzi IP coinvolti, Numero pacchetti, . Generalmente eseguito in locale , in quanto è difficile raccogliere router-level prop(problemi di accesso da remoto). . E' il più difficile da realizzare tra i livelli di analisi.
- Packet trace e flow-level data (livello centrale): volume dei dati ancora grande : i router raccolgono informazioni sui flussi di pacchetti e li salva. Siccome i pacchetti sono molti si tiene traccia di pacchetti prelevati a campione. I packet traces possono essere ottenuti in diversi punti della rete ma non remotamente per i privilegi d'accesso
- Application-level data (livello più alto): piu semplice, implementata con il loggin. I dati possono essere raccolti in qualsiasi locazione.

Cap.5 INFRASTRUCTURE QUIIIIIIIII

5.1 Proprietà fisiche dell'infrastruttura internet:

- Dispositivi fisici: links, routers, wireless.
  Link : Le performance associate ai link sono : Packet delay, Packet loss e Jitter (Descritti anche nelle pagine precedenti).
  Router: ricevono pacchetti in entrata e li instradano all' esterno (mediante buffer e coda). Ci sono diverse tecniche di misurazione, per avere info sul traffico, possono esserci diverse risposte in base alle richieste ricevute :
  L'architettura dei router (configurazione) rende differenti le risposte su tempi di misurazione. Il tempo per rispondere ad un messaggio ICMP può ad esempio differire dal tempo necessario per il forward di un pacchetto (tempi diversi di processazione pacchetti).
  I router hanno due proprietà di interesse : statiche e dinamiche.
  1. Propr. Statiche: indirizzi IP utilizzati dal router, locazione geografica dei router.
  2. Propr. Dinamiche: tempo impiegato per le risposte (messaggi, instradamento pacchetto).
  Wireless: La scelta del wireless "crea" problemi quali: distanza per ricezione segnale, affidabilità, possibili interferenze ecc.
  Esistono diverse tecnologie wireless , che applicate alle misurazioni pongono l'attenzione su vari aspetti, come ad esempio: potenza segnale, data bit rate, copertura , ecc.
  Molto spesso le complicanze sono date anche da cross-traffic, ovvero la separazione del traffico che proviene dalla rete wired rispetto a quello che proviene dalla rete wireless.

Per quanto riguarda l'infrastruttura topologica invece:

- Topologia della rete:
  (Autonom System descritti precedentemente)
  - Grafi AS: i diversi AS presenti nella rete vengono collegati da archi per lo scambio di informazioni e nell'insieme formano un grafo .
  - Router graph: All' interno di un As ,i router sono organizzati in un insieme di locazioni fisiche, dette Point of Presence (PoPs), ovvero uno o piu router in una singola locazione. Il Router graph da una visione dettagliata dell' organizzazione dei vari router. E' un grafo in cui i vertici sono router e gli archi i collegamenti tra loro
  - Intreface graph: le interfacce dei router sono i nodi(vertici) e gli archi i collegamenti.

- Proprietà fisiche riguardanti il traffico:

  - Ritardo dei pacchetti (packet delay): Il ritardo di un pacchetto dipende da diversi tempi dovuti alla trasmissione e al trasporto.
    Il tempo speso all' interno del router si suddivide in tre "sottotempi":

1. Packet processing delay: Caratterizzato dal tempo impiegato dal router per determinare qual è l'interfaccia uscente del prossimo next of router. (ritardo proporzionale alla taglia del pacchetto)
2. Queuing delay: Tempo speso in coda Fifo.
3. Additional delay: Ritardi dovuti a vari fattori (fallimento di instradamento)

Per il packet delay si considera inoltre:

- il Transmission Delay, ovvero il tempo richiesto per posizionare un pacchetto su un link. (se un pacchetto ha taglia 's' ed il link ha capacità 't' , allora il trasmission delay è uguale ad s/t.)
- il Propagation Delay, ovvero il tempo richiesto dal pacchetto per passare da un end di un link a quello successivo (misurato in millisecondi).
(se un link ha lunghezza fisica 'd' , con segnali propagati con velocità 'v' , il propagation delay è uguale a d/v.)

IN GENERALE LA SOMMA DI TUTTI I RITARDI DEVE ESSERE MINIMA (EVITARE ALTA CONGESTIONE E QUINDI ALTO PACKET LOSS(CODA PIENA, PACCHETTI SCARTATI).

- Pacchetti persi: si verifica quando un pacchetto viene scartato, corrotto o rifiutato (congestione). Si utilizza il packet loss rate per misurare il numero di pacchetti persi. Non è sempre possibile sapere il momento esatto in cui un pacchetto viene perso. In generale un packet loss può essere caratterizzato come un "time series of counts"(meno preciso, conto ma perdo l'attimo), si mantiene il conteggio su un timescale. (se Cn è il numero di pacchetti che entrano nella reta al tempo n ed Ln è il numero di pacchetti persi durante questo periodo, allora il packet loss rate può essere definito come : Ln/Cn.)
- Throughput: quantità di dati trasmessi in una unità di tempo. E' importante sapere che se ho una serie di hop (link in serie), il throughput finale è dato dal link con minima capacità (link che rappresenta il collo di bottiglia)
- Jitter dei pacchetti: variabilità dei tempi con cui i pacchetti arrivano. L'ipotesi migliore è che la variabilità sia quanto più vicina allo zero, o comunque molto bassa. In questa caso, posso evitare , quasi sempre, i burst di traffico (quantità di traffico molto alta(traffico elevatissimo), su piccolissimi timescale.) (es. rilascio di un nuovo prodotto: milioni di utenti si collegano (rilascio apple)).
  I burst di traffico (simili ad attacchi Dos) non sono prevedibili , così potrebbero far crashare i server. (es. Attacchi alle torre gemelle).
  Dunque se i tempi di interarrivo sono molto bassi, il traffico è regolare altrimenti no. Bisogna essere in grado di intervenire immediatamente.

5.2. Problematiche (challenges)

Poniamo delle domande:

1) Data una lista di ASes, esiste un tool che da in output la topologia di internet? **NO.**
2) Dato un path da una sorgente ad una destinazione, esiste un tool che può determinare quanto tempo impiega un pacchetto per raggiungere la destinazione? **NO.**
3) Dato un insieme di router lungo il path di un pacchetto esiste un tool che può determinare i ritardi introdotti da ciascun router? **NO.**

La risposta è data da una serie di problematiche descritte(anche) in precedenza -> riepilogo:

- Semplicità nel progetto dei router con approccio stateless. Questo approccio ha come svantaggio la mancata osservabilità in diversi punti della rete. router “stupidi” che non hanno memoria ma si occupano solo dell’ instradamento (per ottimizzare performance).
- Il modello a clessidra dei protocolli di rete ha come protocollo di trasmissione IP, il che nasconde i dettagli degli strati inferiori (tecnologie di connessione dei dispositivi es. ethernet, bluetooth ecc). Nello specifico se si fanno misurazioni sul packet capture, in caso di sniffet di pacchetti, non si è in grado di capire la differenza tra due link sottostanti.
- Middleboxes: Siccome alcune funzionalità complicate devono essere fornite dagli end system, per lasciare il core della rete , il più semplice possibile(end to end argument). Esistono degli elementi che possono violare però il principio end to end e sono detti middleboxes. I middleboxes sono:
    - Firewalls: bloccano il traffico indesiderato e analizzano la semantica delle connessioni.
    - Traffic shapers: scartano pacchetti a seconda del traffico
    - Proxies: terminano le connessioni all’interno della rete, migliorano le prestazioni.
    - NAT: C’è un indirizzo unico, dietro c’è una rete interna , mappata su differenti porte. Modificano gli indirizzi IP dei pacchetti in transito, ottimizzando l’uso dello spazio di indirizzamento. Il NAT è stato introdotto per risolvere il problema della scarsità di indirizzi IP (IPV4).

  Tutti questi elementi causano problemi nel campo delle misurazioni del traffico internet: Vengono nascoste le connessioni agli altri indirizzi IP nella sottorete, ovvero viene nascosta l’architettura (tipologia) della rete, in quanto si vede un solo nodo per un ping ad un determinato indirizzo IP.

- Barriere Amministrative: Un’ altra challanges importante, molti amministratori non vogliono dare info sulla loro rete interna: configuraizone router, traffico gestito, ecc. bloccando quindi le info a questi dati.

5.3. Tools

I tools vengono utilizzati per varie funzioni, come ad esempio il network measurement.

Misure della rete: La misurazione richiede dispositivi sia HW che SW. Le misurazioni sono di tipo:

- attivo se di tipo intrusivo, aggiungono traffico alla rete per effettuare misurazioni.
- passivo se non sono intrusive, sniffano i dati attraverso tecniche di sniffing.

Tool di misurazione attivi, (aggiungendo traffico alla rete allo scopo di effettuare misurazioni)

- Ping: permette di misurare il tempo impiegato da un pacchetto per andare e tornare dal server

- Traceroute: utilizzato per determiare il path seguito dal pacchetto da sorgente a destinazione.
  Il traceroute utilizza il campo TTL (Time to live) dell' header IP:
  il TTL è il max numero di hop che il pacchetto può attraversare, ad ogni passaggio poi ogni router decrementa, fino ad arrivare a 0, dove viene mandato un pacchetto di destinazione non raggiungibile.
  Presenta un insieme di problematiche:
  -Asimmetria dei path: il forward path può essere diverso dal reverse path.
  -Path non stabili e archi falsi:
  -Risoluzione di alias:
  -Carico delle misurazioni aggiunto da traceroute: il problema si presenta in due varianti; traceroute da una singola sorgente a più destinazioni oppure da sorgenti multiple a singola destinazione.

Tool di misurazione passiva: effettuata tramite varie tecniche (non si aggiunge ulteriore traffico sulla rete) :

- BGP: per capire il traffico in ogni AS è necessario ottenere le BGP tables da tutti gli AS le quali forniscono informazioni parziali circa la topologia dell'AS. Lo scopo è quello di costruire una routeviews repository che collezione le tabelle BGP.
  Vantaggi: grandi sistemi AS-AS e router-router possono essere studiate analizzando le tabelle
  Svantaggi: alcune connessioni potrebbero non essere mostrate

- OSPF: usato per ottenere misurazioni passive all'interno di AS tramite la raccolta di dati relativi agli announcements (LSA) in un routing domain. Misurazione utile per comprendere la topologia di un router graph all'interno di un AS.

- SNMP: interroga i MIB (Management information base) dei device, i quali forniscono varie informazioni sui dati in entrata e uscita dei dispositivi. I risultati vengono inseriti all'interno di un DB

Misurazione combinate: L’active measurement richiede una grande quantità di dati per il probe, per limitarla è possibile combinare la misurazione attiva con quella passiva attraverso l’accesso alle BGP dell’AS.

Capitolo 6. Traffic

Le misurazioni e modellazioni del traffico vengono effettuate per analizzare le prestazioni della rete e ingegnerizzare quest'ultima.

6.1 Properties

Quali sono le proprietà base del traffico internet che bisogna misurare?
Bisogna innanzitutto catturare i pacchetti su link o router, poi attraverso i processi stocastici viene riportata l'analisi del traffico osservato.

La misura del traffico più comune è data dal numero di bytes che i pacchetti in arrivo nel nodo contengono.
Si può salire come astrazione, descrivendo la struttura del traffico come il risultato di una collezione di processi ON/OFF. (Se c'è un' attività sulla rete è On, altrimenti Off)
I processi on/off, possono causare problematiche di performance in quanto creano burst.
Esistono tre livelli di attività ON/OFF:
Livello più basso : ci sono i processi.
Livello superiore: i pacchetti formano "trains" di pacchetti da sorgente a destinazione.
Livello più alto: c'è l'intera sessione.
Ad ogni livello quindi i dati vengono sempre più aggregati.

Un altro modo per analizzare dati è quello di prendere flussi di pacchetti:
Flusso: insieme di pacchetti che attraversano il punto di osservazione nel periodo di tempo. Sono caratterizzati da pacchetti con caratteristiche comuni.

IP flow: un insieme di pacchetti riconosciuti tramite l'indirizzo IP

Network flow: insieme di pacchetti che entrano in una rete nel periodo di tempo ed escono da un altro punto. Si prende in considerazione una rete sorgente ed una destinazione, anziché prendere un IP specifico.

6.2 Challenges

Le problematiche della misurazione del traffico sono sia pratiche che statistiche. Nel dettaglio:

- Pratiche:
  - Osservabilità: i router non mantengono informazioni, ogni punto ha una visione locale del traffico e delle proprietà della rete
  - Volume dei dati: più veloce sono i link maggiori sono i dati al secondo da dover conservare.
  - Condivisione dei dati: il traffico contiene dati sensibili degli utenti, i quali per privacy non possono essere prelevati e dunque ciò è in contrasto con le misurazioni
- Statistiche:

- Long tails e alta variabilità: i dati sono altamente variabili e semplici statistiche non sono realistiche.
- Stationarity e stability: Stabilità= consistenza del traffico nel tempo. Analizzare alcuni eventi, dipende dal tipo di analisi che si vuole svolgere. In generale il traffico risult essere quai sempre stabile (eccezione picchi)
- Autocorrelation and memory in system behaivor: In qualche modo il sistema tiene memoria della storia passata. code molto lunghe comportano un dilatamento dei tempi per svuotarle, ciò comporta una autocorrelazione nel comportamento del sistema. Il comportamento corrente è simile a quello di un passato recente.Si più quindi subire un degrado di Performance.

6.3 Tools

I tool per l'analisi catturano i pacchetti e sono divisi in categorie:

- Packet Capture su General Purpose Systems:
  un endsystem può memorizzare i pacchetti che attraversano l'interfaccia di rete. Le Api utilizzate sono libpcap, per catturare i pacchetti . I software utilizzati per il parsing di header fields e analisi dei protocolli sono
    Tcpdump: usato per debug di applicazioni di rete per determinare se gli instradamenti avvengono correttamente.

    Wireshark: packet sniffer che permette all'utente di osservare il traffico sulla rete, simile a tcpdump ma con interfaccia grafica.

- Packet Capture su Special Purpose Systems:
  Il monitoring di core network links richiede hardware specializzato e bisogna consentire accesso fisico per la copia dei dati. Software usati all'interno di backbone sono :
  - OC3MON
  - OC12MON

- Control Plane Traffic:
  Ha come obiettivo il controllo del traffico durante lo scambio di messaggi BGP di routing

- Data management (problema di gestire i dati): il full packet capture e storage presentano problemi su link ad alta velocità, per questo scopo si usano tools specializzati (es. Gigascope , tool che genera query in GSQL ed accede a porzioni di traffico interessate, che appunta limita in finestra il traffico che ci interessa(quanità minimale, alias Data reduction)).

- Data reduction: tratta il problema della riduzione dei dati da processare. I metodi comuni sono:

  - Traffic counters e collezione di flussi di record: i router contano i bytes o pacchetti per unità di tempo. I packet trains sono record che conservano diverse informazioni sul traffico per monitorarlo.
  - Modelli basati su Sampling
  - Modelli probabilistici

Il traffico viene analizzato su piccoli o grandi timescale, per quelli piccoli si utilizza il **modello stocastico** (modello matematico su dati casuali). Su lunghi timescale il traffico presenta variazioni predicibili,è possibile differenziare il traffico su fasce temporali.

Self similarity model: nel caso in cui si possiede una memoria a lungo termine che conservi i valori delle misurazioni si nota che i più recenti sono correlati a valori di istanti passati.

Modello di poisson: genera traffico bursty (poca trasmissione e molta inattività) su scale brevi e genera valori omogenei su scale lunghe.

6.4. Risultati più importanti riguardo il traffico internet

In generale, se c'è necessita di misurare su lunghi timescale(maggiori di un'ora), non ci sono problemi eccessivi, con tante possibilità di analisi.
Su piccoli timescale invece, come detto non esistono variazione predicibili, per questo si usano i processi stocastici(insieme ordinato di variabili casuali indicizzate dal parametro t(tempo)), in quanto l'analisi del traffico risulta essere più complicato. I processi stocastici hanno il comportamento dello scaling behaviors, ovvero se si va a scalare il timescale di un fattore m, si ottiene il traffico al fattore t x m, ovvero ottengo periodi piccoli che non fanno overlapping tra di loro. Lo scaling behaviors può essere dunque descritto in termini di 2 fenomeni, sulla quale si basa il traffico internet:

- Long Range Dependence (LRD):
La LRD indica caratteristiche di irregolarità del traffico, che si presentano identiche indipendentemente dalla scala adottata. Se esiste un comportamento in un dato timescale, questo comportamento sarà uguale anche su scali differenti (sia più grandi che più piccole). Si parla perciò di self similarity del campione corrispondente.
Il traffico telefonico è risultato basarsi su modelli che si basano su traffico indipendente, quindi può essere modellato con processi stocastici indipendenti(Poisson). Al contrario, il traffico internet mostra correlazione, ci sono fluttuazioni con comportamenti identici al variare del timescale. Se c'è correlazione, significa che non può esserci indipendenza, quindi il traffico internet non può essere modellato con modelli indipendenti come i processi di Poisson. Tutto ciò significa che il modello per il traffico telefonico non è ASSOLUTAMENTE VALIDO PER IL TRAFFICO INTERNET.

- Self similarity:
Si parla di "Qualcosa che sembra essere smile indipendentemente dalla scala". L'idea è che c'è qualcosa che si ripete , su scala differente(def. Di frattale). Il modello di Poisson genera un traffico bursty , se osservato su

scale piccolissime (millisecondi), se la scala cresce, questa caratteristica si perde. Al crescere della scale i picchi vengono smussati da un' operazione di media su una scala sufficientemente grande.

Nel 1993 ci furono una serie di ricercatori che dimostrarono che il traffico sulle reti LAN , segue un comportamento Self Similar.
Il concetto di Self Similarity è stato per questo "collegato" alle misurazioni di traffico.
Se prendiamo un router per le misurazione, prendendo i seguenti timescale :
- 1s , 100ms, 10ms
Se prendeiamo Network Traffic e Poisson Traffic:
Poisson: su piccoli timescale mostra traffico bursty, man mano che il timescale aumenta, il traffico si appiattisce.
Network: su grandi timescale il traffico è bursty, come d'altronde lo è se aumentiamo i timescale (Self similar model).

In sostanza il traffico internet non segue un modello di Poisson, in quanto LRD e Self Similarity, contribuiscono a rendere il traffico di tipo Bursty, su tutte le scale.
Questo aspetto risulta essere fondamentale per poter progettare le componenti di rete, per un traffico non predicibile.
Ne seguono 10 osservazioni: (slide da 82 a 91 lezione del 21/10/2020 da minuto 24 a minuto 27 della registrazione.)
1) Il traffico internet continua a cambiare e crescere su piccoli timescales.
2) Il traffico aggregato è self similar (o frattale).
3) Il traffico di rete esibisce la proprietà di locality.
4) Il traffico non è uniformemente distribuito attraverso gli host della rete.
5) La distribuzione della taglia dei pacchetti è bimodale.
6) Il session arrival process è di tipo Poisson.
7) Il packet arrival process non è di tipo Poisson.
8) La maggior parte delle conversazioni sono brevi.
9) I Flussi di traffico sono bidirezionali ma asimmetrici.
10) Il protocollo TCP è il più usato su internet.
Questi modelli formulati nel 2008, valgono tutt'oggi.