RETI TELEFONICHE

Circuit switching: end to end resources reserved for a call, guaranteed performance, no sharing, call setup required, full link bandwith

TECNOLOGIA FISICA DELLE RETI

Actually, two network (transport and control).

Pachet switching: multiplexing (STM relation between time slot and user, telephone; TDMA slot-user dynamic, no store-and-forward; ATM independent packets, store-and-forward, efficent for bursty traffic)

COMMUTAZIONE DI CIRCUITO VS COMMUTAZIONE DI PACCHETTO

Pachet switching allows more users to use network, great for bursty data, simplex: no call setup, sharing, excessive congestion: delay, loss, protocol needed.

STRUTTURA DI INTERNET

Dumb network, host intelligent. Store-and-forward: entire racket must arrive at router before it can retransmitted on next link.

Longer packet leads to a lower overhead but result in a higher chance to be corrupted and must be retransmitted, causing congestion.

Roughly hierarchical, network of networks.

Tier-2: regional ISP

Ritardo di accodamento ABC con BC più lento di AB

NodalDelay=ProcessDelay+QueuingDelay+TransmissionDelay+PropagationDelay

TrafficIntensity=PacketLenght*AveragePacketArrivalRate/LinkBandwidth

When packet arrives to full queue, packet is dropped (lost)

T=PacketLength/LinkBandwidth+TransmissionDelay

CALCOLO TRASMISSIONE PACCHETTI

STACK ISO/OSI

Application(FTP, HTTP, CBR)/Transport(TCP,UDP)/Network(IP,RIP)/Link(PPP,Ether)/Physical

Implemention reliability in the network may produce undesirable effects for apps (VoIP)

LINK LAYER

Inoltro diretto e indiretto con netmask: occorre verificare se il pacchetto appartiene alla sottorete di una delle interfacce: AND bit a bit tra indirizzo dell'interfaccia e netmask, e tra indirizzo dst e netmask, se i due risultati coincidono allora è la stessa e si procede con l'inoltro diretto.

Se il confronto da esito positivo per più righe della routine table si sceglie quella con netmask con più 1 (prefisso più lungo)

SWITCH Store and Forward se 2 ingressi richiedono lo stesso cammino si ha congestione (risolvo con datagrammi o VC)

VIRTUAL CIRCUIT all'inizio della comunicazione ho RTT per decidere il VC.

A invia setup alla rete con indirizzo di B ogni switch che riceve il setup crea una nuova connessione nella tabella

VC scegliendo un VCI non assegnato e lo inoltra allo switch dopo verso B; Quando B riceve il setup, invia conferma ad A segnalando il VCI scelto, ogni switch scrive nella tabella in VCI ricevuto e lo inoltra scrivendo il

proprio VCI scelto fino ad A.

SPANNINGTREE Root-> id basso, porta root più vicina alla radice, scelgo brige più vicini a radice e blocco in

dati le altre porte per eliminare i loops, ogni nodo manda frame config (id.nodo, id.root, distanza):

Il nodo 2 manda (2,2,0) se riceve (1,1,0) cambia il suo messaggio in (2,1,1) e lo inoltra.

Se un nodo riceve due messaggi da 2 nodi più vicini alla radice di lui blocca la porta di quello minore se la distanza è >1, altrimenti blocca entrambe.No scalabile.

INDIRIZZAMENTO IPV4

Indirizzi a 32bit (2^32). NetID-HostID.

Classe A ([0]8bit di NetID, 0.0.0.0-127.255.255.255); Classe B ([10]16bit di NetID 128.0.0.0-191.255.255.255); Classe C ([110]24bit di NetID192.0.0.0-223.255.255.255); Classe D ([1110]Multicast); Classe E ([1111]future use).
Privati: 10; 192.168 ; 172.16-172.31

SUBNETTING E SUPERBNETTING

HostID=0 identifica la rete; =255 è broadcast diretto; tutto1=broadcast limitato alla sola rete.
NetID=0 host sulla stessa rete del mittente; tutto0 =quando il mittente non conosce il proprio IP.
Loopback=127
Classful:scarsa flessibilità,pochi indirizzi;sub/supernetting,Classless,NAT
Subnetting con netmask, suddivido un indirizzo di classe C (>24)
Supernetting con netmask (<24)

NAT traduzione indirizzi di rete, i pacchetti inviati su internet non possono avere indirizzo src o dst locale, router NAT ha tabella di traduzione. Host A richiede pagina web esterna, assegna una porta e manda il datagramma al router, il router genera un nuovo numero di porta di origine (non presente in tabella NAT), mette il suo indirizzo e inoltra al sever. http risponde a quella porta, il router cerca nella tabella la corrispondenza e converte il datagramma, Supporta 60,000 connessioni con un solo IP.Contestato per uso improprio numeri porte, elaborazione oltre al livello 3, viola argomento end-to-end.

ARP

IP Unico formato,univocità,indipendenza fisica; Routing,frammentazione, tipo di servizio, ip->mac, messaggi errore icmp, connection less, best-effort, incapsulamento.
L'host chiede a tutti chi è l'ip xxx e l'ip xxx riceve il mess e risponde all'host il suo mac address.
Tabelle con corrispondenza IP-MAC. Se non c'è l'entry nell'ARP-CACHE viene generata un'ARP-Request in broadcast, l'host che riconosce il suo IP invia un'ARP-Reply con il suo MAC.

PROXY ARP

Usato per evitare la configurazione del default gateway o routing table negli host.
Permette di raggiungere host su lan diverse.
RARP non più usato per assegnare indirizzi IP(no netmask e solo se su stessa lan) (ReverseARP)
BOOTP (porta 67/68) livello applicativo (client/server UDP, passive open)
DHCP (porta 67/68) livello applicativo (client/server UDP): client invia DHCPDISCOVER in broadcast con il proprio MAC; il server risponde con DHCPOFFER con l'IP proposto;client accetta l'offerta con DHCPREQUEST e il server conferma con DHCPACK con le info per la configurazione (ip, netmask, gateway, dns server).
Il client rilascia con DHCPRELEASE

TRANSPORT

Collegamento logico tra app su host remoti. Gestisce più app con (de)multiplexing usando le porte (0-65535) i numeri noti (o-1023) sono assegnati a server, lato client numeri dinamici.
IndirizzoIP+Porta=socket

UDP Unreliable, unorder delivery.Best-effort, connectionless, loss tolerant, rate sensitive, max 65507 (maxi p= 2^16 -1 meno 20headerIP+8headerUDP) Header:src port, dst port, checksum, length. IP Data into UDP packet

TCP Reliable, in-order delivery.Congestion contro,flow control, connection setup, error recovery, reordering.All byte sent are recived.Full duplex,handshake, pipelined, segmentation.
Chechksum su tutto mentre IP solo su intestazione.
MSS=segment size;MSIZE=message size;C=link rate;W=outstanding segments
Stop-and-wait:A send, B recive and send ACK, A send …W=1 Throughput=MSS/(RTT+MSS/C)
Go-back-N: always send ACK for correctly-recived packets with highest (in-order) seq#
Out-of-order packet are discarded and reACK. Resend at timeout RTT.
Thr=min(C,W*MSS/(RTT+MSS/C))
Continuous transmission W*MSS>RTT*C
Selective repeat: individually ACK for correctly-recived packets, sender resent only unACK packets.

TCP Packet into IP Data.
Karn's problem: not distinguish among an ACK of the original segment and to a duplicate.
Not update RTT whean a segment has been retransmitted because of RTO expiration or exponential backoff. When ACK resume RTT.
Fast retransmit: Timeout long, if sender recive 3 dupACK for the same data=retransmit.

FLOW CONTROL

Se l'app è lenta nella lettura può accadere che il mittente mandi in overflow il buffer di ricezione inviando i dati troppo velocemente.
Reciver advertise spare room by includine value of RcvWindow in segments, sender limits unACKed data to RcvWindow (no bufferoverflow).
Deadlock: persist timer, sender transmits probe, exponential backoff.
ADVERTIZED WINDOW B segnala ad A che è pieno con un ACK(0) a si ferma e continua a mandare probe (evita stallo) NAGLE: se ha dati meno di MSS e B ha spazio lo manda solo se i pacchetti precedenti sono stati
inviati con successo(invia quando arriva conferma).
Silly-window:il buffer si svuota lentamente e il mittente manda pacchetti da 1 byte. Sol=il ricevitore manda update solo se buffer è min(1/2 recived buffer size;MSS)
Nagle=Mittente manda prima porzione di dati anche se corta, gli altri solo se il buffer di uscita =MSS o se ACK.
Threehandway handshake SYN, SYNACK, ACK. MSS in SYN (DoS)
TearDown: FIN, ACK, FIN, ACK TIME_WAIT

CONGESTION CONTROL

Il livello di rete non fornisce supporto esplicito al livello di trasporto per il controllo della congestione la cui presenza deve essere dedotta dai sistemi terminali, in base all'osservazione del comportamento della rete(perdita pacchetti, ritardi..)
In parole povere se il mittente TCP si accorge di condizioni di scarso traffico incrementa il proprio tasso trasmissivo e viceversa.
End-to-end (no network feedback, inferred from loss and delay,TCP), use a second windows when timeout or 3 dupACK.
Slow-start: start with small cwin (1 MSS) and increase linearly when ACK; when lost restart (or threshold max(min(cwin,win)/2; 2MSS)))
Fast recovery: cwin=1/2 cwin, window grows linearly; after timeout cwin=1 MSS
Throughput= 0.75*W/RTT
Se RCWND<CWND RTT=2tau+MSS Thr=W/RTT con W=RCWND*MSS in bit
CALCOLO DEL FAIR-SHARE
Network-assisted (feedback by routers)
CONGESTION WINDOW (cura la congestione)Decremento Moltiplicativo: mando al max MaxWindow=min(CW,AW) ad ogni timeout spirato dimezzo CW fino a 1; Incremento Additivo: CW=CW+1 (uno
ogni RTT) quando ACK dell'intera finestra arriva, all'inizio CW=1; Slow-Start:(incrementa di uno per ogni ACK
ricevuto) CW=CW+1 quando ACK singolo arriva partendo da CW=1, quando ho congestione fisso CW all'ultimo
numero e riparto con Incremento Additivo, se perdita di nuovo Slow-Start e mi fermo a CW/2; Ritrasmissione Veloce: invio ACK duplicati, al terzo ACK uguale mando il pacchetto e non riparto con Slow-Start.
A-1->B-ack1->A
A-2->B-ack2->A
A-3-x… … ..
A-4->B-ack2->A
A-4->B-ack2->A
A-5->B-ack2->A-3->B-ack6->A
TCP Tahoe: Slow start, Congestion avoidance, Fast retransmit
TCP Reno: Opening up congestion window after fast retransmit,Delayed acks
DISTANCE VECTOR Informazioni scambiate tra routers [indirizzo dst, distanza], DV inviato

solo ai nodi adiacenti, periodicamente, stima distanze con Bellman-Ford distribuito. Facile, lento, loop, poco stabile su grandi reti, count to infinity: rappresentazione infinito con valore finito > cammino critico.
Split-horizon: se A manda a B pacchetti destinati a X, non ha senso che A annunci a D con quale costo raggiunga X o Poisonous Reverse: manda il mess di tutte le destinazioni ma pone a INF quelle raggiungibili da quel link.(non funziona su certe topologie)
Hold-Down: dopo notifica che rete non raggiungibile ignora gli update per 60s.
Triggered Update: cambi di topologia annunciati immediatamente e distinti, più veloce a scoprire guasti. Il nodo avverte in caso di costo di path non corretto.
DISTANCE VECTOR ogni nodo conosce i vicini e la distanza, locale, ogni nodo comunica ai vicini la sua informazione e si aggironano, problema count2infinity, split-horizon dovuto ad un ciclo.
LINK STATE Ogni nodi impara le distanze dei vicini e invia a tutti le info (flooding LSP), tutti i nodi costruiscono la mappa completa e si calcolano i cammini minimi con Djikstra. Più flessibile, invio solo dopo cambiamento, veloce. Protocollo dedicato per vicini, flooding, riscontro pacchetti, difficile.
Se il LSP non e`mai stato ricevuto, o il SN e`superiore a quello in memoria: mem LSP, flooding
Se il LSP ha lo stesso SN: ignora. Se il LSP e`piu`vecchio, ritrasmette quello piu`recente al mittente. Il nodo avverte in caso di costo di link non corretto.
LINK STATE ogni nodo determina i vicini e trasmette la sua informazione a tutta la rete, globale, ogni nodo determina il cammino minimo con dijkstra,ho flooding risolto con aging.
(IDnodo, elenco vicini diretti e costo collegamento,#seqenza,TTL) uso Dijkstra.
RIP Il protocollo RIP è stato uno dei primi protocolli di instradamento 1982. Poi IETF introduce la seconda versione RIP 2, la quale presenta la possibilità di trasportare un numero maggiore di informazioni, senza rendere obsoleta la versione precedente.V1=DistanceVector, 16=INF, incapsulati in UDP porta 520. Loop,low infinity, convergenza lenta, solo hop cout, solo un cammino per destinazione, no autenticazione, lunghezza definita da UDP. Limitato a piccole network
V2=Autenticazione, subnetmask,multicast 224.0.0.9
Il tipo di metrica usata è l'Hop count e gli Updates, che contengono l'intera copia delle routing table, vengono scambiati ad intervalli regolari (ogni 30 secondi) e quando si verificano dei cambiamenti nella topologia. Tutte le volte che un router riceve un update che contiene entry modificate, deve aggiornare la propria routing table incrementando di 1 l'Hop count e indicare come next hop l'indirizzo IP del router da cui ha ricevuto il messaggio. La tabella di routing indicherà, per ciascuna entry della tabella, solo il percorso migliore per raggiungere la destinazione desiderata. Una volta che è stato aggiornata la routing table, il router trasmetterà immediatamente un update per informare gli altri router adiacenti dei cambiamenti. In questo particolare caso, gli updates vengono inviati senza attendere i 30 secondi di default.
Ciascun router, in una rete nella quale opera questo protocollo, viene considerato come 1 hop. Se un router apprende un percorso verso una certa destinazione che richiede il passaggio di altri tre router, scriverà nella propria routing table in corrispondenza della suddetta destinazione, un Hop count = 3.
L'indirizzo IP di destinazione è forse il campo più importante contenuto nella routing table. Infatti quando un router riceve un pacchetto dati attraverso la sua porta di IN, controlla nella propria tabella di routing se esiste una entry per tale destinazione, ed in caso affermativo inoltra il flusso dati nella corrispondente porta di OUT.
Il campo next hop contiene l'indirizzo del router successivo verso il raggiungimento della rete di destinazione.
Per quanto riguarda il Timer, il RIP deve scandire temporalmente ogni quanto inviare gli updates ad i router vicini, inoltre considererà irraggiungibile un router vicino se da questo non riceve notizie almeno una volta ogni 180 secondi.
Una caratteristica da non trascurare è che il Protocollo RIP 1 non invia le subnet mask ma solo gli indirizzi IP, di conseguenza possono verificarsi degli errori in quanto non vengono riconosciute eventuali sottoreti. Questo problema viene risolto nella versione RIP 2, infatti è presente nel

pacchetto un campo chiamato subnet mask che contiene appunto la subnet mask corrispondente alla entry considerata. In aggiunta questa versione fornisce un semplice meccanismo di autenticazione per rendere più sicuri gli updates delle routing table.
Un ulteriore differenza fra RIP 1 e RIP 2 riguarda i messaggi di updates; nel primo caso essendo tali messaggi di tipo broadcast si può verificare un sovraccarico nella rete e un tempo di convergenza lento, mentre per quanto riguarda il secondo i messaggi vengono inviati in multicast, interessando così solo certi router, alleggerendo così il numero di informazioni da trasmettere.
OSPF Routing gerarchico, protocollo Hello, identificativo univoco router, LinkStateAdvertisement, ToS metrics(throughput, delay…), incapsulati in IP.
Area border router diffondono in ciascuna area un riassunto delle info raccolte nell' altra area.
Point-to-point (2 router), Transient link (rete a cui sono connessi vari router), stub link (rete ad unico router),virtual link (admin).
ESERCIZIO TOPOLOGIA
LSA Tipo1:router link adv (LSP); Tipo 2:network link adv(pseudo nodo DR lan); Tipo 3: summary link to net adv (area border router);Tipo 4:summary link to AS border router(area border router, indica la presenza di AS boudary router nell' area e il costo)
BGP Come DV ma intero percorso (TCP) Se ne percorso ricevuto c'è l'AS di cui fa parte lo scarta per non creare cicli. permette VPN, specifica percorso con lista di AS attraversati
DNS UDP Resolution, reverse resolution, alias, mail servers, voip.
Distribuited hierarchical database. Recursive query refused by root and TDL: iterative query.
HTTP Stateless (cookies on client side), TCP, 1.0 new connection for each object referenced in html (2RTT): 1.1 non new connection, no slow-start, fewer RTTs. Proxy:web caches.
CDN Simple caching (client-side proxy)
FTP Separate control/data connection (out-of-band), stateful control.
EMAIL SMTP (TCP): handshaking, transfer, closure.
POP3: no organized in folders, no flag management, needs client polling.
IMPA:push email notification, extendable, flag, organization, complex.
P2P
Serverless communication, without any central entity. Scalable, resilient, free.
Problems:consensus, reliability, NAT, anonimity, security.
TCP e UDP,new node join (bootstrap).
Centralized (Hybrid), Hierarchical (Supernodes), Pure (unstructured, query by flooding.max hops, no NAT, high overhead).
DISTRIBUTED HASH TABLE
Each node ID=H(rand); user wants to publish a file "the_matrix.avi": H(file)=k1, H("matrix")=k2, H("the")=k3, H("avi")=k4. Publish key:k1, value: <ip> and key:k2-4, value: H(file) "the_matrix.avi". Distance bucket: key in closest bucket (ID similar key).
Suffers hot-spots. No security.
CHORD Scalable, routing table O(log(N)), O(log(N)) message for lookup.
KADEMLIA Distance metric: ID XOR key, O(log(N)), resilient to DoS, old node more stable, scalability, XOR easy, queries keep routing table up-to-date. Difficult implementation, hot-spots.
P2p is aggressive, parallels TCP streams, offers service similar to ISP but free, bandwith.
Requires traffic classification: port based (simple, dumb); payload, statistical and behavioral analysis,
MULTICASTING
Se supporto si manda un solo pacchetto e i router sono attivi. IGMP mandato periodicamente dal router e gli host rispondono con l'elenco dei gruppo a cui appartengono.
Join e Leave. DV per costruire l'albero dei cammini minimi.
Pochi router su internet sono multicast=MBone tunneling
SICUREZZA
Integrità, confidenzialità, controllo accessi, autenticazione

Meccanismi non crittografici deboli: IP, nonces, controllo accessi mediante firewall.
Attivi, passivi sniffing.
DoS: TCP SYN con indirizzi src fasulli per far allocare la banda al server.
CRITTOGRAFIA SIMMETRICA Chiave privata, chiavi sufficientemente lunghe e casuali.
CRITTOGRAFIA ASIMMETRICA Chiave pubblica
RSA n=p*q, z=(p-1)*(q-1), e*d=1(mod)z P=(e,n), S=(d,n), M'=M^e(mod n), M=M'^d(mod n)
Firma Sa(M)->Pa(Sa(M')) ma il mess non è crittato, Pb(Sa(M))->Sb(Pa(Sa(M'))) troppo costoso; Diffie-Helmann:
A invia g^xmodn, B invia g^ymodn, B calcola (g^xmodn)^ymodn A calcola (g^ymodn)^xmodn che sono uguali.m+MD5(m+k)+Sa(k)
MANINTHEMIDDLE A->g^xmodn->T->g^zmodn->B->g^ymodn->T->g^zmodn->A
AUTENTICAZIONE: A-idA,DES(x,Ka)->B-DES(x+1,Kb), DES(y,Kb)->A-DES(y+1,Ka)->B-DES(Kab,Kb)A; oppure A-RSA(x,Pb)->B-x->A
FIRMA DIGITALE:A-M'=RSA(M,Sa)->B-M=RSA(M,Pa)
HASH f:X->Y f facile da calcolare avendo x, x difficile da calcolare avendo f, difficile da trovare un valore x' con
f(x)=f(x')
Integrità e autenticazione m+MD5(m+Kab)
WEP Non sicura, uso improprio primitive crittografiche: spazio IV troppo ristretto per garantire poche collisioni (4000 pacchetti per pcollisione=50%). Si può desumere il keystream relativo a coppia IV,Key senza conoscere Key.
WPA WPA2 migliore, AES ma non supportato da router=TKIP miglioramento di WEP ma sempre vulnerabile
FIREWALL DMZ: regole firewall per server, diverse dalle regole della rete LAN.
MOBILE IP UDP nodo mobile che arriva in una nuova rete deve apprendere l'identità dell'agente di quella rete passivamente con agent advertisement o attivamente con richiesta in broadcast. Il nodo mobile riceve il COA(lista di uno o più indirizzi fornita dall'agente ospitante) e sceglie uno di questi indirizzi inviando un mess di registrazione IP all'ospitante. L'ospitante protocolla l'IP permanente del mobile ed invia un mess di registrazione al domestico. Il domestico controlla autenticità e correttezza, associa l'IP permanente del mobile al COA da lui selezionato. E manda risposta all'ospitante che a sua volta risponde al mobile con la risposta di registrazione. Domestico data scadenza. Non serve chiusura.