

metti trasmittivi: Fisico (cavo coaxiale), Guidati (twisted pair, fibra ottica), A onda libera

trasferimento dati attraverso la rete: commutazione di circuiti (circuit switching CS: la banda è divisa in pezzi, in base alla frequenza (frequency multiplexing division FMD) o al tempo (time multiplexing division TMD)) o di pacchetto (packet switching PS: non esiste più un "canale" ma solo i dati da inviare. Questi vengono divisi in pacchetti che poi sono lanciati nella rete senza preallocazione di risorse (cioè senza setup). Ciascun pacchetto occupa completamente il canale durante la trasmissione. Avviene una multiplexazione statistica. Qui c'è la possibilità di accodamento e di perdita di pacchetto).

struttura di internet:

Internet Service Provider (ISP) di livello 1 (internazionali), 2 (nazionali e distrettuali), 3/vocali (di accesso).

Ritardi nel trasferimento di pacchetti:

- 1. di elaborazione } nel nodo
 - 2. di Accodamento
 - 3. di trasmissione: L/R } sulla linea
 - 4. di propagazione: d/s }
- con L: lunghezza pacchetto (bit), R: freq. trasmissione del collegamento (bit/s), d: lunghezza del collegamento fisico, s: velocità di propagazione nel collegamento ($2 \cdot 10^8$ m/s)

Throughput: $\frac{\text{bit totali trasmessi}}{\text{tempo di trasmissione}}$

Goodput: $\frac{\text{bit utili trasmessi}}{\text{tempo di trasmissione}}$

tempo totale di trasmissione di un singolo pacchetto attraverso 3 interfacce e 2 router

$$3 \cdot tp + 3 \cdot \frac{H+L}{C} + 2 \cdot te + 2 \cdot ta =$$

(4 router) tempi di accodamento

tempi di propagazione (4 interfacce che attraversano) $\rightarrow \# \text{interfaccie}$

$$= \sum_{i=1}^N \left(\frac{H+L}{C_i} + d_{\text{prop},i} \right) + \sum_{j=1}^{N-1} \left(d_{\text{elab},j} + d_{\text{mem},j} \right)$$

ritardi interfaccia ritardi nodo

con hp:

- tempi di propagazione uguali su tutte le interfacce
- C uguale su tutte le interfacce (questo spesso non è vero)
- tempo di elaborazione uguali in tutti i nodi (verosimile)
- tempo di accodamento uguale in tutti i nodi (spesso non vero, molto variabile)

tempo di trasferimento di flusso interruttivo immesso in rete a pacchetto:

CASO PACCHETTI A DIM COSTANTE:

$$D = d_{\text{prop},B} + \frac{H+L}{C} N + \frac{1}{C} \left\{ \left[\frac{X}{L} \right] (H+L) \right\} - \frac{H+L}{C}$$

ritardo di prop. ritardo ritardo su 4 ritardo ritardo
TOTALE SU 4 trasmissione trasmissione
N interfaccia 4 pacchetti 4 pacchetti 4 pacchetti
4 pacchetti attraverso necessari a attraverso attraverso
N interfaccia trasferire 4 interfaccia
il messaggio

CASO PACCHETTI A DIM VARIABILE $\leq L_{\text{MAX}}$:

$$D = d_{\text{prop},B} + \frac{H+L_{\text{MAX}}}{C} N + \frac{1}{C} \left\{ \left[\frac{X}{L_{\text{MAX}}} \right] H \right\} - \frac{H+L_{\text{MAX}}}{C}$$

ritardo di prop. ritardo ritardo su 4 ritardo ritardo
TOTALE SU 4 trasmissione trasmissione
N interfaccia 4 pacchetti 4 pacchetti 4 pacchetti
4 pacchetti attraverso necessari a attraverso attraverso
N interfaccia trasferire 4 interfaccia
il messaggio

$$\text{con } L_{\text{MAX}} = \sqrt{\frac{H \cdot X}{N-1}}$$

Modello OSI open System Interconnection descrive l'architettura di una rete con 7 strati.

1. FISICO
2. DI COLEGAMENTO
3. DI RETE
4. DI TRASPORTO
5. DI SESSIONE
6. DI PRESENTAZIONE } uniti nel modello di internet
7. DI APPLICAZIONE }

Lo strato n in un sistema interagisce lo strato n in un altro sistema per fornire servizio allo strato n+1.

Le entità di strato n si scambiano unità dati dette PDU.

Lo strato n+1 trasferisce le proprie informazioni invocando il servizio dello strato inferiore (n). Ogni strato passa le informazioni allo strato inferiore fino a che si raggiunge lo strato fisico che si occupa dell'effettivo trasferimento.

Le unità dati ricevute da uno strato e provenienti dallo strato superiore sono dette SDU.

$$SDU + \text{Header} = n+1 \text{ PDU}$$

strato fisico:

- informazione a blocchi: definita dalla size in byte
- informazione stream: definita dal flusso di bit (bit rare)

$$\text{delay minimo} = t_{\text{prop}} + \frac{L}{R} = \frac{d}{v} + \frac{L}{R}$$

con d: lunghezza collegamento
c: vel. prop. su mezzo trasmissivo
L: bit trasmessi (riducibile con compressione)
R: vel. trasmissione Sorgente

(riducibile con trasmissione compression: senza perdita (MPEG)/con perdita (JPEG))

$$\text{compression rate } R_c = \frac{B_{\text{orig}} [\text{bit}]}{B_{\text{compr}} [\text{bit}]}$$

digitalizzazione segnali analogici:

1. campionamento
2. quantizzazione (errore di quantizzazione: se si comette associando il campione al valore del livello più vicino)
3. compressione

Teorema del campionamento: una trasmissione analogica può essere rappresentata nel dominio della frequenza in base al suo dominio di freq. (freq min e max, larghezza di banda dei segnali), e la freq. di campionamento minima per rappresentare fedelmente il segnale è $F_c = 2W_s$ con W_s la larghezza di banda del segnale.

bitrate $R_s = \# \text{bit}/\text{sample} \cdot \# \text{sample/sec}$

↳ segnale analogico campionato

informazione stream: può essere di tipo constant bit rate o variable bit rate; la sua qualità segue i parametri di delay, jitter, loss.

trasmissione:



Conversione flusso informativo prodotto da sorgente in segnale adatto a trasmissione

transmission impairments:

1. attenuazione del segnale
2. distorsione del segnale
3. rumore additivo
4. interferenza con altri segnali

Se la trasmissione analogica è a lunga distanza si usano una serie di ripetitori (amplificatore + equalizzatore) che puliscono ma la qualità si abbassa comunque: comunicazioni analogiche sono distance limited.

Se la trasmissione numerica è a lunga distanza si usano una serie di rigeneratori che mantengono intatta l'informazione.

Trasmissione ad impulsi: frequenza max di impulsi al secondo $F = 2w_c$ con w_c larghezza di banda del canale. Visto che impulsi/sec è una quantità limitata aumenta i bit/impulso (cioè associa più bit allo stesso impulso).

Trasmissione ad impulsi multilivello: banda: w_c , freq.: $2w_c$ impulsi/secondo, bit rate con 2bit/impulso: $4w_c$ bit/s,

signal to noise ratio SNR:

$$SNR = \frac{\text{potenza media a segnale}}{\text{potenza media rumore}}$$

Limite di Shannon per la banda di un canale: $C = w_c \log_2 (1+SNR)$ bit/s con SNR espresso in decibel

Filtro Passa Basso Ideale: tutte le freq. $f < w_c$ non subiscono alterazione e vengono ritardate di T secondi. Tutte le freq. $f > w_c$ sono bloccate.

Filtro Passa Basso Reale: le freq. sono attenuate in modo diverso e subiscono ritardati diversi.

Filtro Passa Banda: blocca le alte e le basse frequenze

Trasmissione in banda base: se il canale si comporta come un filtro passa basso ideale con w_c larghezza di banda del canale, il massimo rate di trasmissione di una seq. di impulsi è $r_{\max} = 2w_c$ impulsi/sec.

Trasmissione multilivello:

$$r_{\max} = 2w_c \text{ impulsi/sec}$$

$$b = n w_c \text{ bit/sec}$$

$$M \text{ livelli} = 2m \text{ livelli}$$

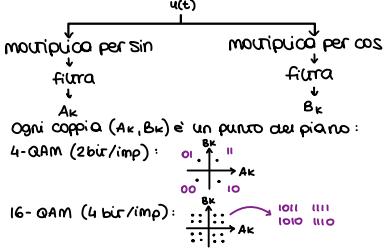
$$\text{bit rate} = 2w_c \text{ imp/s} \cdot m \text{ bit/imp} = 2w_c \cdot m \text{ bit/s}$$

Capacità/limite di shannon: dato un canale con banda w_c e rumore Gaussiano e fissato un valore di S/N in decibel, il massimo rate di trasmissione raggiungibile è:

$$C = w_c \log_2 (1 + S/N) \text{ bit/s}$$

modulazione numerica (traslazione in banda):

- di Amplitude ASK
- di Frequenza FSK (shifta di $\pm f$)
- di Fase PSK (multiplica per cos)
- Quadrature Amplitude Modulation QAM se la banda è limitata la freq max si dimettebbre $F = W_c$ ma usano solo la QAM si possono trasmettere 2 (4,8,...) bit per volta in parallelo. QAM prende coppia di bit, ne moltiplica uno per sin e uno per cos e visto che questi sono ortogonali i risultati possono viaggiare in parallelo. Così facendo posso raddoppiare la frequenza. La composizione viene trasmessa e visto che i due segnali si sommano quando arrivano a destinazione il ricevitore fa il processo di demodulazione 2 volte.



strato di collegamento: (nic)
servizi: framing, rivelazione e correzione errori, controllo di flusso, consegna affidabile di dati, half duplex e full duplex

Framming: Ha lo scopo di formare la PDU al strato (pacchetto) incapsulando la PDU dello strato superiore (pacchettino). Per farlo si aggiungono flag (sequenza fissa e nota da bit: 0111101) a inizio e fine messaggio. Per evitare il problema della similitudine si applicano operatori su di bit stuffing (in emissione: si aggiunge "0" dopo "1") e di bit de-stuffing (in ricezione: dopo 5 "1" consecutivi se c'è un "1" la sequenza è riconosciuta come flag, se c'è uno "0" viene riconosciuto come bit di stuffing e viene eliminato).

Nel protocollo PPP viene usato il bit stuffing (in emissione: se in una parola del frame compare "011110" o "011110" viene premesso un bit "0111101") e de-stuffing (in ricezione: se si ricevono due "0111101" consecutivi uno dei due viene eliminato / se si riceve "0111101" seguito da "011110" il primo viene eliminato / se si riceve solo "011110" viene riconosciuto come flag).

controllo d'errore: due modalità:
Error detection and retransmission (ARQ)
Forward Error Correction (FEC).

blocco da proteggere / **bit di controllo** / **Codeword**
K bit n-K bit nbit
codici con controllo di parità: a parità singola / a parità a blocchi / a ridondanza circolare (CRC)

controllo parità singola: K bit informativi, 1 bit di controllo (se #bit di messaggio è dispari, 0 se #bit è pari). Gli errori sono rilevati solo se sono in numero dispari.
Distanza di Hamming: qualora una codeword è distante da un'altra, si misura in # di bit minimo da cambiare affinché le parole diventino l'altra. Dato d è codice / numero di Hamming, se d è dispari il codice di rilevazione d'errore rileva e corregge 2 errori; se è pari non rileva a/2 e ne corregge (d/2)-1.

Hamming (7,4): 7bit totali, 4 di info, 3 di parità:
dato messaggio 1010
d4 d4 d2 d2 0 d3 d1 d4 0 p4 1 p2 0 p3 1 bit parità
check d4, d2, d4 v x v v v x x 1 = p4
check d4, d3, d4 v x v v x v x 0 = p2
check d2, d3, d4 v v v x x v x 1 = p3

controllo di parità bi-dimensionale:
1. si smuova la sequenza di bit informativi in colonne
2. si aggiunge un bit di parità per ogni colonna
3. si aggiunge una colonna di parità: se modifica un bit di una sequenza informativa si rilevano 2 incongruenze sulla riga e la colonna di controllo che "triangola" l'errore. configurazioni con 1,2,3 errori rilevabili.

interner checksum: data una stringa da proteggere di L byte b_0, b_1, \dots, b_{L-1} di 2^L bit, checksum è una stringa bl di 2^L bit calcolata così:
 $x = b_0 + b_1 + \dots + b_{L-1} \text{ modulo } 2^{L-1}$
 $b_L = -x \text{ modulo } 2^{L-1}$
tale che $0 = b_0 + b_1 + \dots + b_{L-1} + b_L \text{ modulo } 2^{L-1}$

CRC: L'ennesimo bit della stringa da proteggere diventa il coefficiente del termine x^{k-4} del polinomio $P(x)$. Esistente e ragionevole conoscere inoltre il polinomio generatore $G(x)$ ai grado k . Allora vale

$$\frac{x^k P(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$$

viene aggiunto una stringa da proteggere (ϵ di 2^L bit)

Alla fine la PDU emessa ha k (delle della stringa originaria) + ϵ cifre binarie, rappresentative dei coeff. di un polinomio di grado $k+L-1$: $T(x) = x^k P(x) + R(x)$. Tutte le parole di codice sono divisibili per $G(x)$, tutti i polinomi divisibili per $G(x)$ sono parole di codice.

In ricezione, se ci sono stati errori durante la trasmissione, viene risuonato $T(x) + E(x)$ su cui il ricevitore opera divisione per $G(x)$. Segue che resto $\left[\frac{T(x) + E(x)}{G(x)} \right] = \text{resto } [E(x)]$. poiché si aspetta che questo resto sia = 0, il ricevitore si accorge di errori appena resto $\neq 0$ (eccezione: eventualmente che $E(x)$ sia divisibile per $G(x)$). vengono rilevati: errori singoli o doppi, errori isolati con moreplicati dispari, errori a burst di lunghezza $\leq L$.

Protocolli di accesso multiplo:

1. suddivisione del canale \rightarrow TDMA, FDMA, CDMA
2. Ad accesso dinamico controllato
3. Ad accesso dinamico casuale (slotted Aloha, CSMA)

Protocollo Banda Liricato PBR: Rd bit con R=bit rate del metto, d=ritardo di propagazione end-to-end

$$PBR \text{ normalizzato} = d = \frac{R}{P}$$

con L = lunghezza di un frame

Aloha: chi invia trasmette appena ha una frame pronta, chi riceve: manda da sé riceve, oppure nulla. chi invia: se riceve ACK capisce che trasmissione è andata a buon fine, altri magari ritrasmette dopo tempo di backoff.

Intervallo di vulnerabilità: $t_p + t_d$ di frame precedente.
throughput = load · successo
successo = e^{-2t_p}

Slotted Aloha: variante del protocollo Aloha con divisione in time slot e dimensione fissa del pacchetto. si dimezza il tempo di vulnerabilità e raddoppia l'efficienza.

CSMA: un nodo ascolta il canale prima di trasmettere. se trova occupato applica uno di tre algoritmi (-persistenti cioè ascolta con $p=1$, non-persistenti o p-persistenti). A causa del ritardo di propagazione questo metodo non preserva al 100% dalle collisioni. Efficienza: $E = \frac{1}{T + 2D \cdot A}$ con $A \approx e = 2,71$

CSMA-CD: "ascolta prima di parlare e mentre parli". In questo caso la frame ha lunghezza minima tale che la sua trasmissione sia $\geq 2t_{prop} + T_r$ con T_r tempo di janning

ovvero un tempo in cui l'enviatore continua a parlare dopo aver rilevato la collisione per dare a tutti il tempo di accorgersene.

Token passing (accesso dinamico controllato): le prestazioni di questo sistema dipendono dal modo in cui si usa il token:

- **SINGLE TOKEN OPERATION:** il free token è inserito dopo che l'ultimo bit del busy token è tornato ad essere di origine. Ogni frame si porta dietro il token frequency. Per M fino a un certo valore ha efficienza unitaria poi crolla. Il token è sempre e solo uno quindi l'irregolarità si riscontra subito
- **MULTI TOKEN:** free token trasmesso subito dopo l'ultimo bit del frame. un altro viene potrebbe trasmettere subito in coda.

B FRAME, F B FRAME, F ...

Throughput sempre molto alto, tanto più alto quanto più alto è numero di stazioni

- **SINGLE FRAME OPERATION:** il free token è trasmesso dopo che l'enviatore ha ricevuto l'ultimo bit della sua frame. si aggiunge T visto che deve fare tutto a giro. Caso peggiore dei 3, non cambia in funzione di M

Controllo d'errore ARQ:

1. stop-and-wait: A manda frame. Se B lo riceve correttamente invia ACK. Se non lo riceve o se riceve ve sbagliato (contro lo CRC) non manda nulla. Se A riceve ACK prosegue automaticamente il tempo di timeout e poi ritrasmette il frame. Se frame che ricevono sono numerati rispettivamente i valori slast e slast + next (in modulo 2) $t_{out} = t_m$ tempo trascorso fin dall'inizio di un frame
2. $E = \frac{t_{idle}}{t_{total}} = \frac{t_f}{t_f + t_o} = \frac{n \cdot R}{n \cdot R + t_o}$

E diminuisce sia all'aumentare di PBR

2. Go-back N: elimina le arie dei ritorni; il canale è mantenuto occupato inviando altre frame in una finestra di ampiezza W_s con m bit per la numerazione delle frame. Se vengono ricevuti gli ACK (anche cumulativi) delle frame emesse puoi da esaurire la finestra questa si aggiorna (sliding window) e la trasmissione continua, curiosamente la trasmissione si interrompe e viene ripetuta alla scadenza del timeout. Alla scadenza la finestra aggiorna il suo $liminf$ al valore dell'ultimo ACK corretto (Rnext) poiché non accetta frame fuori sequenza.

$$n^* = \frac{t_f}{t_f + t_o} = \text{numero ottimo min di frame consecutive}$$

$limsup \text{ finestra} = slast - ws - 1$

max valore finestra: $ws = M - 1 = 2^m - 1$

Piggybacking: quando la comunicazione tra A e B è bidirezionale le info di controllo sono trasmesse sulla stessa frame delle info utili (se B non trasmette non invia gli ACK ad A che quindi rallenta la sua trasmissione). B può scegliere di trasmettere solo per indicare gli ACK oppure di aspettare per controllare il flusso di A).

E' unidirezionale se la probabilità d'errore è = 0. E' unidirezionale se $ws = to$. E diminuisce al crescere di PBR / ad crescere di Pf: packer loss prob.

3. Selective Repeat: A ritrasmette solo le frame di cui scade il timeout e quelle per cui riceve un NAK. B accetta frame fuori sequenza (che vengono memorizzate in buffer) e fa slittare l'Rnext solo quando riesce a ricostruire la sequenza corretta (con ACK cumulativo).

$$ws + wr = 2^m$$

$E = 1 - Pf$ con Pf : frame loss possibilità

USER DATA PROTOCOL UDP

si: moltiplicazione, demultiplicazione, rivelazione d'errore
no: connessione, controllo di congestione
usato in applicazioni: multi mediali sensibili al bit rate che tollerano piccole perdite o che sono in grado di recuperare l'errore autonomamente (a livello applicativo), usato in protocolli DNS, SNMP, su segmento UDP:

32 bit

PORTA ORIGINE	PORTA DEST
LUNGHEZZA CHECKSUM	Dati dell'applicazione (messaggio)

TRANSFER DATA PROTOCOL TCP

si: connessione, moltiplicazione, demultiplicazione, reliable data transfer, controllo di flusso, controllo di congestione, management di connessione
segmento TCP:

SOURCE PORT	DEST PORT	4 byte
SEQUENCE NUMBER	4 byte	4 byte
ACK NUMBER	4 byte	4 byte
H E R F A S G	W I N D O W	4 byte
C H E C K S U M	U R G E N T P O I N T E R	4 byte
O P T I O N S P A D D I N G	D A T A	N byte

src port e dst port servono per servizi di moltipiaz. e demultipiaz., sequence number e ack number per servizi di reliable data transfer, window per servizi di controllo di flusso, options per negoziare i parametri della connessione

connessione TCP: nuova fase di installazione della connessione le due entità TCP remote si sincronizzano scambiandosi gli identificatori del socket, il proprio numero di sequenza iniziale, il valore iniziale della finestra in ricezione.

Per stabilire la connessione si effettua un THREE-WAY HANDSHAKE:

- HOST A invia un segmento SYN all'host B in cui specifica il num. di seq. iniziale utilizzando nel verso A-B è il MAXIMUM SEGMENT SIZE (MSS)
- HOST B risponde con un segmento SYN ACK in cui allo header specifica il num. di seq. iniziale utilizzato nel verso B-A e la sua MSS
- HOST A risponde con un segmento ACK per liberare la connessione:

- HOST A invia segmento di controllo FIN al server
- HOST B risponde con un ACK
- HOST B chiude connessione e invia un FIN
- HOST A risponde con un ACK
- viene attivato un timer
- HOST B riceve l'ACK e la connessione viene chiusa

controllo di sequenza:

basarsi sui numeri di sequenza (numero del 1° byte del segmento nel flusso di bire), ACK (numero di sequenza del prossimo byte atteso dall'altro host) cumulativi, RTT, retransmission timeout (Rto)

con RTT stimato = $(4 - d) \cdot RTT_{stimato} + d \cdot RTT_{sample}$

RTT stimato: storico del suo valore
RTT sample: l'ultimo suo valore calcolato

d: 0,125

RTO = RTT stimato + 4 * dev(RTT)

dev(RTT) = $(1-\beta) \cdot dev(RTT) + \beta \cdot |RTT_{sample} - RTT_{stimato}|$

$\beta = 0,25$

RTT esponenziale: $RTT_{t+1} = q \cdot RTT_t$

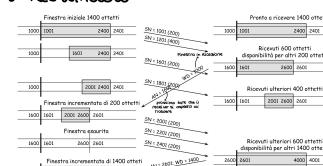
q: 2

controllo di errore:

l'entità TCP emittente può rivelare precocemente i segmenti perduti tramite l'analisi degli ACK duplicati (che indicano un segmento smarrito). Se l'entità TCP emittente riceve 3 ACK duplicati per lo stesso dato suppone che il segmento che segue quello riscontrato sia perso. A questo punto non attende lo scadere del timer ma applica la rimessione rapida. FAST RETRANSMIT

controllo di flusso: il controllo di flusso ha lo scopo di limitare il ritmo di emissione dei dati da parte di un host per evitare la saturazione delle capacità del buffer in ricezione. TCP utilizza un controllo di flusso che opera a livello di byte, basato su una finestra scorrevole di larghezza variabile e sui seguenti parametri:

- Sequence Number SN
- Acknowledgement Number AN
- Rec Window



THROUGHPUT DI CONNESSIONE:

TH = tempo di trasmissione utile in un RTT =

$$RTT = \min \left[1, \frac{w}{2a} \right] = \begin{cases} 1 & \text{se } w \geq 2a \\ \frac{w}{2a} & \text{se } w < 2a \end{cases}$$

con w: larghezza in byte finestra

in trasmissione

c: birete connessione

d: ritardo propag. su connessione

Cd: PBR

a: ca espresso in bire

controllo di congestione:

In TCP il controllo di congestione è di TIPO PUNTO - PUNTO: la congestione è declara osservando perdite e ritardi nei sistemi terminali e sfruttando 3 meccanismi:

- esaurimento RTO come sintomo di congestione
- finestra di congestione (Congwin) che si affianca alla finestra di ricezione imponendo una limitazione addizionale alla quantità di traffico che un host può inviare in una connessione

- sgoggia (threshold) il cui valore è pari alla metà della congwin al momento in cui viene rilevata una perdita. All'inizio della connessione (slow start) è posta = +oo
L'entità emittente determina nel tempo il valore della finestra disponibile (Available Window Awain) che indica il numero di segmenti di lunghezza max MSS che possono essere inviati senza riscontro. Awain $\leq \min(Congwin, Recwin)$

ADDITIVE-INCREASE MULTPLICATIVE - DECREASE

aumenta congwin finché non si verifica una perdita. L'aumento è additivo, cioè aumenta di 1 MSS a ogni RTT senza perdere, e il decremento è moltiplicativo, cioè riduce congwin alla metà dopo una perdita.

Per evitare congestione l'emittente TCP segue una procedura ciclica in due fasi:

- slow start:
Quando inizia la connessione congwin = 1 MSS, soglia = +oo. La frequenza aumenta in modo esponenziale fino a quando non si verifica una perdita. Allora congwin(new) = 1 MSS, soglia = congwin(old).

2 congwin raddoppia a ogni RTT.

- congestion avoidance: se c'è aumento che si ha nella fase slow start raggiunge e supera il valore di soglia, cioè congwin > soglia, l'incremento di congwin diventa lineare al crescere di RTT, e questo incremento continua, finché i riscontri arrivano prima dei loro rispettivi RTO, cioè fino al raggiungimento della saturation su uno dei collegamenti lungo il percorso o in uno dei nodi attraversati

Recap:

- quando congwin < soglia l'emittente è in fase slow start
- quando congwin > soglia l'emittente è in fase congestion avoidance
- quando si verificano 3ACK duplicati soglia = congwin/2, congwin = soglia
- quando scade RTO, soglia = congwin/2, congwin = 1 MSS

Emulazione: funziona esattamente come la realtà, la subisce, dà un'idea dell'andamento.

Simulazione: è basata su modelli matematici, calcola i tempi di un certo avvenimento poiché non subisce direttamente la realtà come un emulatore. È un software che non replica la realtà ma la modella.

Router: device dello strato di rete, è un commutatore multiporta; riceve pacchetti (u.i. dello strato di rete) e li smista alla porta di uscita corretta tramite la routing table

Routing Table: può avere una configurazione statica o può seguire un protocollo di routing definito in modo dinamico. Serve per ri lanciare il pacchetto verso una destinazione che non è su una delle reti a cui è connesso il router. È composta da tuple <IP dts; IP next hop; ID porta di uscita; info statistiche>

Indirizzo IP: indirizzo a 32 bit o 4 byte che identifica un'interfaccia di rete. Può assumere notazione decimale puntata cioè 4 numeri ognuno da 0 a 255 separati da un punto. L'IP è composto da NetID e HostID, ed è affiancato da una maschera di sottorete che specifica il numero di bit dell'IP che fanno parte del NetID. Data un NetID, dai possibili indirizzi che si possono creare variano l'HostID, due vanno considerati "speciali": quello con i bit di HostID tutti posti =1 (che prende il nome di indirizzo Broadcast) e quello con i bit di HostID tutti posti =1 restano quindi utilizzabili 2ⁿ⁻² host con n=bit di HostID. L'IP ha valenza globale.

Indirizzo MAC: indirizzo binario a 48 bit, assume notazione a 6 cifre espresse in esadecimale separate da trattino, ogni cifra rappresentante 8 bit. È assegnato alla scheda di rete al momento della fabbricazione e la identifica univocamente. Il MAC ha valenza locale.

ARP: ARP è un protocollo che avviene internamente ad una LAN e serve a determinare il MAC di un'interfaccia conoscendone l'IP. Un host manda un ARPRequest in broadcast chiedendo il MAC corrispondente all'IP esplicitato nella richiesta, e riceve una risposta unicast dall'host che si è riconosciuto con tale IP. Il primo host allora salva tale MAC nella sua ARPTable (una in ogni host/router della LAN, contiene tuple <IP; MAC; TTL>).

ARP tra LAN diverse: hostA vuole comunicare con hostB su un'altra LAN. È consapevole che hostB è su una LAN esterna alla propria perché già conosce l'IP di hostB e quindi tramite il NetID sa di essere su una sottorete differente. Allora la ARPRequest sarà incapsulata in una frame Ethernet che ha come MAC sorgente quello di hostA e come destinazione il MAC del Next Hop, cioè un'interfaccia del designated router. hostA emette in broadcast la richiesta, il router si riconosce come destinatario e quindi apre la frame, ispeziona il pacchetto IP decapsulato e identifica l'IP di destinazione (che è quello di hostB). Allora il router ri lancia il messaggio dalla porta corretta (routing table), solo quando la richiesta raggiungerà hostB verrà aperta, e hostB emetterà la sua ARPrepy.

Ethernet: è una tecnologia "wired" per la configurazione di LAN. Può avere topologia bus (superata), o star (a stella, prevalente ai giorni nostri). Usa come u.i. la frame Ethernet, che incapsula il pacchetto IP dello strato di rete, formata dai campi: preamble (8 byte), addresses (6 byte per indirizzi MAC di src e dst), type, data, CRC.

Switch: device dello strato di collegamento, ha un ruolo attivo in quanto, senza bisogno di configurazione (self learning), immagazzina e ri lancia frame Ethernet esaminando il MAC delle frame entranti e selezionando quali ri lanciare e come, utilizzando il CSMA/CD e la Forwarding table.

Forwarding Table: tabella presente in ogni switch, le cui entry sono tuple <host MAC; interfaccia per raggiungere tale host; TTL>. La tabella è inizialmente vuota (e finché lo switch non ha completato il processo di apprendimento per inviare le frame usa flooding). Lo switch impara quale host può essere raggiunto tramite quale interfaccia tramite l'indirizzo src delle frame che riceve.

Man In The Middle: Trudy (l'intruso) forza lo switch a mandargli messaggi non indirizzati a lui ma ad un hostB e convince l'host emittente hostA che la comunicazione con hostB sia andata a buon fine in quanto risponde ad hostA fingendosi hostB
ARP Cache Poisoning: è realizzabile solo all'interno di un'unica LAN. L'avvelenamento avviene sia su hostA che su hostB, emettendo ARP false che ri portano al MAC di Trudy

Subnetting: con la configurazione IP=NetID+HostID il numero di host sarebbe limitato. Si opera quindi subnetting: alcuni dei bit di HostID diventano bit di subnetID che identificano la sottorete a cui appartengono gli host definibili tramite i bit rimasti nell'HostID. La subnet mask identifica i bit che compongono i campi NetID+subnetID.

Classless Inter Domain Routing CIDR: ad una rete è assegnato un certo numero di blocchi contigui di indirizzi (supernetting), identificato da un unico prefisso. Questa modalità rallenta la crescita della dimensione delle routing table.

Strato di rete: due funzionalità: Forwarding (data plane), routing (control plane). Il control plane può essere strutturato con un controllo per-router distribuito (algoritmi di routing di tipo link state per ogni singolo router, che hanno come output la scrittura di una routing table, questa modalità necessita della conoscenza della rete) o con un controllo centralizzato (una sola entità calcola le routing table e i router eseguono, riducendo le loro funzioni a quelle di uno switch. L'instradamento ha una gestione più efficiente).

Protocolli di routing: possono essere di tipo link state (presuppongono la conoscenza completa della topologia di rete. Si basano sul algoritmo di Dijkstra, per cui vale il principio di ottimalità dei sottopercorsi) o di tipo distance vector (i router conoscono solo i vicini a cui sono direttamente collegati, e si basano su processi iterativi di scambio di informazioni con questi ultimi. Si basano sul algoritmo di Bellmann-Ford per cui il percorso minimo da x a y è basato sul calcolo del minimo, calcolato tra tutti i vicini v di x, della somma del path da x a v + il path tra v e y. Vale il principio per cui le buone notizie viaggiano veloci, le cattive notizie viaggiano lentamente)

Sistema Autonomo AS: aggregato di router. Intra-AS routing svolto da Interior Gateway Protocols IGP (es. RIP, OSPF, IGRP); inter-AS routing svolto da Border Gateway Protocols BGP (protocollo in due parti: eBGP per ottenere informazioni sulla raggiungibilità di sottorete dai s. vicini basato su advertisement del tipo <AS Path; prefisso della destinazione> ri lanciati dai border router, e iBGP per propagare informazioni di raggiungibilità a tutti i router all'interno dell'AS) per cui non è necessaria la conoscenza della topologia di rete. Nel BGP, se vengono trovati più path per raggiungere un AS esterno, il migliore viene scelto tramite criteri di shortest AS-path o di closest next-hop (tramite l'Hot Potato Routing)