1 Physical Layer

$C = 2B\log_2 M$ $\quad SNR = \frac{P_r}{N_0 B_c}$ $\quad C = B_c \log_2(1+SNR)$ $\quad \frac{P_t}{P_r} = \frac{(4\lambda f d)^2}{c^2}$

2 Data Link Layer

$FER = 1-(1-BER)^n$

i Error Probability: $P = \binom{n}{i} p^i (1-p)^{n-i}$

Stop and Wait

$$S_{max} = \frac{T_f}{T_f + 2\times T_{prop}} = \frac{1}{1+2a} \quad S = \frac{1-p_e}{1+2a}$$

Go Back N

$$W = M-1 = 2^k - 1$$

Efficiency: (%)

- If $W \geq 1+2a \Rightarrow S = 1$.
- If $W < 1+2a \Rightarrow S = \frac{W}{1+2a}$.

Efficiency with Errors:

$$S = \begin{cases} \frac{1-p_e}{1+2ap_e} & ,W \geq 1+2a \\ \frac{W(1-p_e)}{(1+2a)(1-p_e+Wp_e)} & ,W < 1+2a \end{cases}$$

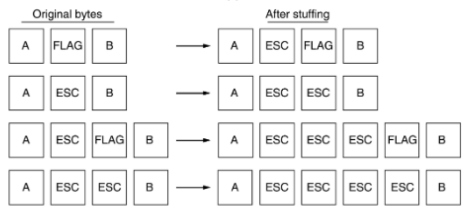
Selective Repeat

$$W = \frac{M}{2} = 2^{k-1}$$

$$S = \begin{cases} 1-p_e & ,W \geq 1+2a \\ \frac{W(1-p_e)}{1+2a} & ,W < 1+2a \end{cases}$$

Byte Stuffing

- Inserting a special escape byte (ESC) before each flag byte in the data.
- Makes framing flag bytes distinguishable from the ones in the data.
- Escape bytes present in the data also need to be escaped.



Useful Formulas for All Methods

$$T_f = \frac{L}{C} \quad R_{max} = S \times C$$

$$T_{prop} = \frac{d}{V} \quad a = \frac{T_{prop}}{T_f} \quad Deb_{max} = R_{max} \times S_{max} \quad RTT = 2\times T_{prop} + T_f$$

Reliability in the TCP/IP

Capacity of one link $C_l = C*(1-PLR)$

End to End capacity

» using Link-by-Link ARQ: $C_{LL} = C_l = C*(1-PLR)$

End-to-end ARQ ➔ **Inefficient when PLR is High**

» Using End-to-End ARQ: $C_{EE} = C*(1-PLR)^K$

3 Delay Models

3.3 Statistical Multiplexing

$$T_{frame} = \frac{L}{C}$$

- Packets of all traffic streams merged in a single quele (first-come, first-served)

3.4 Frequency Division Multiplexing

$$T_{frame} = \frac{Lm}{C}$$

- Link capacity C subdivided into m portions
- Channel bandwidth W subdivided into m channels of W/m Hz
- Capacity of each channel = C/m

3.5 Time Division Multiplexing

$$T_{frame} = \frac{Lm}{C}$$

- Time axis divided into m slots of fixed length
- Communication -> m channels with capacity C/m

3.6.1 M/M/1 Queue

- Poisson arrival
- Exponential service time
- Time Division Multiplexing

$$T_W = \frac{\rho}{\mu(1-\rho)} \quad N = \frac{\rho}{1-\rho} = \frac{\lambda}{\mu-\lambda}$$

$$N_W = N - \rho \quad T = \frac{1}{\mu-\lambda} \quad P(n) = \rho^n(1-\rho)$$

M/M/1/B Queue

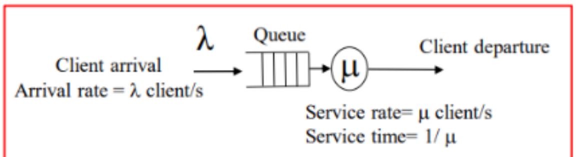
- M/M/1 queue has limited capacity (B buffers)
  - » Packets can be lost
  - » Probability of packet being lost = P(B) ➔ Queue is full
- Analysis similar to M/M/1

$$\sum_{i=0}^{B} P(i) = 1 \qquad P(n) = \rho^n P(0)$$

$$P(0) = \frac{1-\rho}{1-\rho^{B+1}} \qquad P(B) = \frac{(1-\rho)\rho^B}{1-\rho^{B+1}}$$

- Particular cases

$$\rho = 1, \quad P(B) = \frac{1}{B+1} \qquad \rho >> 1, \quad P(B) \approx \frac{\rho-1}{\rho} = \frac{\lambda-\mu}{\lambda}$$



Important Variables and Expressions

λ — arrival rate - pacotes processados na porta de saída (pac/s)

μ — service rate (pac/s) $\quad$ (bit/s) $Debito = \lambda \times L$

N — Average number of customers/packets in the network

T — Average delay per packet -> waiting plus service times (μs)

ρ — traffic intensity (occupation of the server) $\quad \rho = \frac{\lambda}{\mu}$

$T_{pac(frame)}$ — Service time = packet transmission time

L — tamanho médio de cada pacote (bit) $\quad T_{pac(frame)} = \frac{L}{C} = \frac{1}{\mu}$

C — capacidade da porta (bit/s)

T_W — average waiting time

N_W — average number of clients waiting

3.6.2 M/D/1 Queue

Used when packets have constant size.

$$T_W = \frac{\rho}{2\mu(1-\rho)}$$

3.6.3 M/G/1 Queue

$$T_W = \frac{\lambda E(T^2_{pac(frame)})}{2(1-\rho)}$$

4 MAC Sublayer

4.4 Channel Partitioning

Divide channel into smaller "pieces"(time slots,frequency).

Poor efficiency on low loaded channels.
The principle protocols are:

- Time Division Multiplexing;
- Frequency Division Multiplexing.

4.5.6 Taking-turns protocols

Tightly coordinate shared access to avoid collisions.
Usage of the communication resource is disciplined by some turning mechanisms.

- Each station has its own turn;
- Stations with more information to send, might have bigger turns;
- **Polling:**
  - Controlled by a master station which invites slave stations to transmit in turn.
- **Token passing:**
  - The stations will pass the control token from one station to next sequentially, warning which is able to transmit.
  - **concerns**: token overhead; latency; single point of failure (token).

4.5.3 CSMA (Carrier Sense Multiple Access)

Carrier-sense multiple access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium.

- When a collision happens the station waits random time and repeats algorithm;
- Collision vulnerability time = 2*Tprop;
- Collision probability = a = Tprop/Tframe;

4.5.5 CSMA with Collision Avoidance (CSMA/CA)

Carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be idle. When they do transmit, nodes transmit their packet data in its entirety. It is an unreliable method

- To avoid channel capture, station waits random backoff time between two consecutive frame transmissions, even if the medium is sensed idle in the DIFS time.
- **It uses ACKs.**

4.5 Random access protocols

- Each station tries to access the full communication resource in a random, uncoordinated manner -> collisions occur;
- Poor efficiency on highly loaded channels;
- When station has packet to send a packet,transmits at channel data rate **R** bit/s.

4.5.1 Pure ALOHA

Aloha is a technique for coordinating the access of large numbers of intermittent transmitters in a single shared communication channel.

- In Aloha, whenever a station has data, it transmits it;
- If more than one frames are transmitted, they collide and are lost. The Sender finds out whether the transmission was successful or experienced a collision by listening to the broadcast from the destination station;
- If ACK (signal that data has been received successfully) not received within timeout, then a station picks random backoff algorithm to re-transmit;
- After the backoff time, the station re-transmits the frame.

4.5.2 Slotted ALOHA

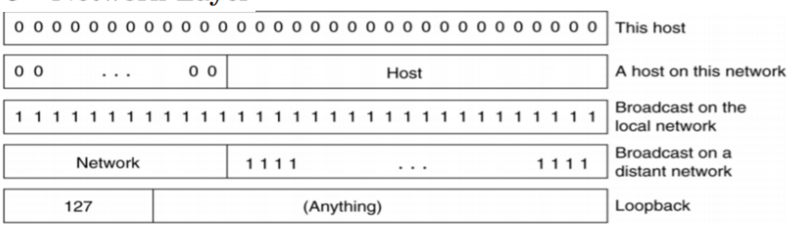
In the Slotted ALOHA, the time is divided into time slots and each slot corresponds to one frame.
A station is not permitted to send whenever the user types a line. Instead, it is required to wait for the beginning of the next slot and the stations transmit frames only at the beginning of a time slot.
This method causes a reduction on the collision probability.

4.5.4 CSMA with Collision Detection (CSMA/CD)

CSMA/CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA/CD immediately terminates the transmission thus shortening the time required before a retry can be attempted. The last information can be re-transmitted.

- **Carrier Sense:** Station senses medium before transmitting. If free, station starts transmission. If busy, waits until its free and then transmits (= 1-persistent)
- **Collision Detection:** If collision is detected,the transmission is aborted and the re-transmission is delayed using a Binary Exponential Back-off algorithm.
- **Binary Exponential Back-off algorithm:**
  - Time is modeled in time slots and each Tslot= 2*Tprop;
  - After the i consecutive collision -> waits a random number of slots uniformly distributed in [0, 2i-1] and attemps to re-transmit.
- **Doesn't use ACK.**
- To detected a collision,**Tframe>2*Tprop**.

5 Network Layer



Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

5.11 NAT - Network Address Translation

- Permite que cada computador tenha um IP interno numa rede, sendo o IP externo diferente

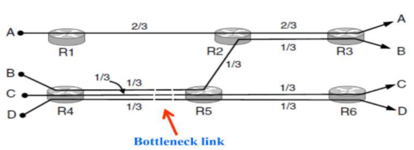
5.12 ICMP - Internet Message Control Protocol

- Usado pelo router ou host para mandar mensagens de erro ou de controlo (como o ping)

6 Transport Layer

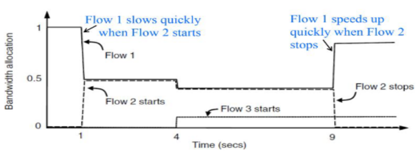
6.23 Max-min fairness

Fair use gives bandwidth to all flows (no starvation)
» **Max-min fairness** gives equal shares of bottleneck



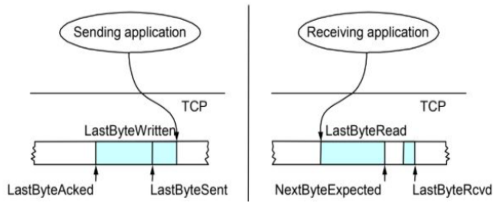
6.24 Bitrates along the time

Bitrates must converge quickly when traffic patterns change



Sliding Window

- Sender
  - LastByteAcked < = LastByteSent
  - LastByteSent < = LastByteWritten
  - Buffers bytes between LastByteAcked and LastByteWritten
- Receiver
  - LastByteRead < NextByteExpected
  - NextByteExpected < = LastByteRcvd +1
  - Buffers bytes between LastByteRead e LastByteRcvd



Flow Control

- Buffer length
  - Sender → MaxSendBuffer
  - Receiver → MaxRcvBuffer
- Receiver
  - LastByteRcvd - LastByteRead < = MaxRcvBuffer
  - AdvertisedWindow = MaxRcvBuffer -(LastByteRcvd - LastByteRead)
- Sender
  - LastByteWritten - LastByteAcked < = MaxSendBuffer
  - LastByteSent - LastByteAcked < = AdvertisedWindow
  - EffectiveWindow = AdvertisedWindow - (LastByteSent - LastByteAcked)
- Sending application blocks if it needs to write y bytes and
  - (LastByteWritten - LastByteAcked) + y > MaxSenderBuffer
- Slow start phase:
  - increase exponentially fast (despite name) at connection start, or following timeout
- congestion avoidance:
  - increase linearly