

Telemática

Apuntes de Pak (Fco. J. Rodríguez Fortuño) ETSI Telecomunicación. Universidad Politécnica de Valencia. Segundo cuatrimestre de 3^{er} curso Curso 2005/2006

Contenido

- Apuntes extensos con problemas
- Enunciados de examen, algunos resueltos

Fecha de última actualización: 30 Marzo 2008

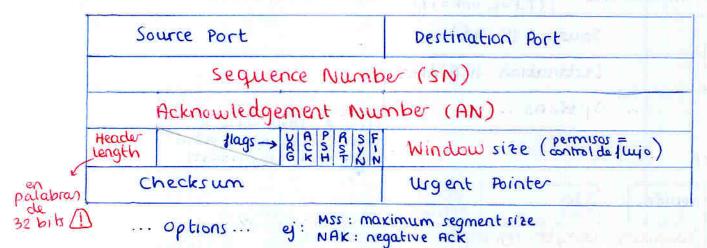
Telemática

4 en pal	abraz de 11 [5-15]		
Version Head		Total length	(en bytes)
Identification (todos la	n is tragmentor iqual)	OLL Fragment	Offset
Time to Live	Don bo col	Header Check	rum
So	wa IP Address		Jack Jumac
De	stination IP Address	22	
	tions	Clase A Ored, h. Clase B 10 red, re Clase C 110 red. Clase D 1110 (,	d.h.h red.red.h
	the Flow Lo lass (Identifi	ibel (20 bits)	(79
Payload Le	ingth (en bytes)	Next Header (yai final: Protocol)	Hop limit
an malanka s	, r. Unite indica		
		dress (128-bit)	
	Source Ada		
detran lan co	Source Ada	dress (128-bit)	

UDP:

Source Port	Destination Port
Total Length (enbyten)	Checksum (opcional)

TCP:



Ambos añaden, pora calcular el checkrum, una pseudocabecera

4	- 32 bits -	
IP	origen	
IP	destino	
ceros	Protocolo F1 = 0 P =	Longitud to tal de dalagrama UDP o segmento TCP

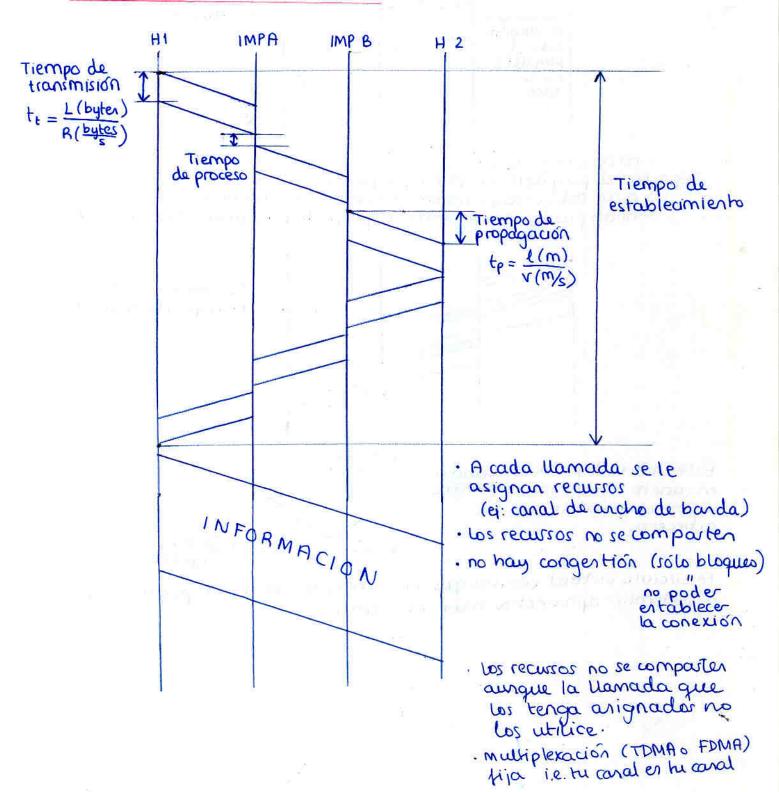
1. Ambito

LAN: local: uso privado, en general multipunto

WAN: wide: público, en general punto a punto MAN: metropolitan: interconectar LAN's a alta velocidad GAN: global: interconectar WAN a MUYalta velocidad

2. Estructura de juncionamiento

2.1. Conmutación de circuitos



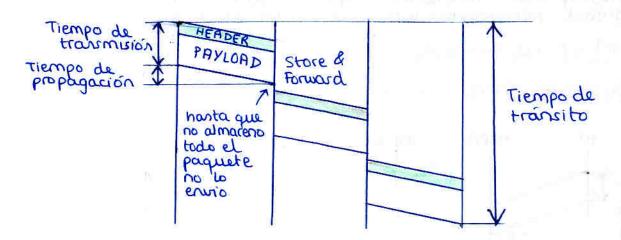
2.2. Conmutación de paquetes

· flujo de datos se divide en paquetes · store « forward

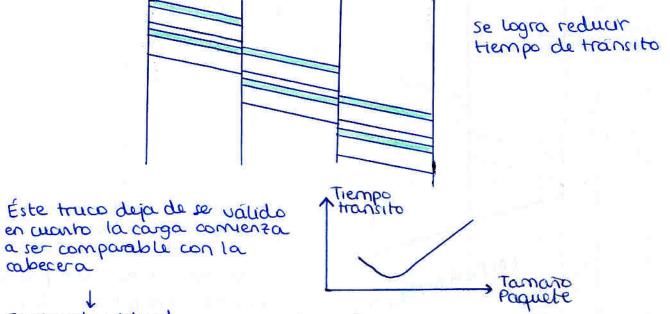
estadística (secuencia de paque tes sin patrón (1/3)

cada paquete se transmite al total de ancho de banda del enlace. recursos se utilizar en función de las necesidades » puede excederse.

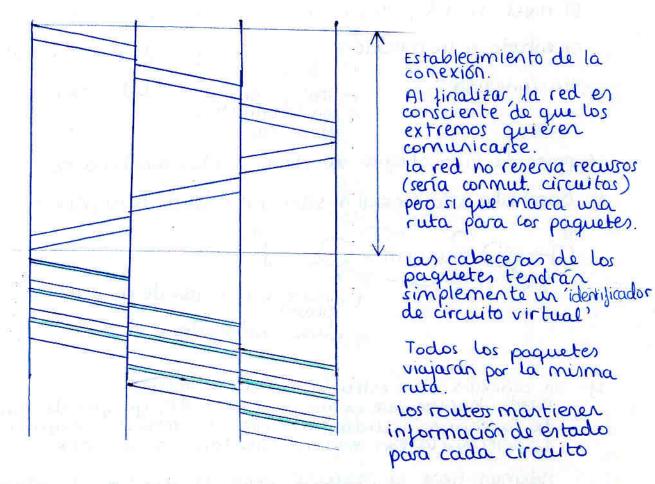
Conmutación de paquetes tipo datagrama co



* tamaño paquetes:
Repartir el payload en mái paquetes:
-mái cabeceras: mayor tiempo transmisión
-nodo puede ir enviando 1º paquete mientras llega el 2° Dvs.



En circuito virtual veremos que las cabecaras son mas pequeñas y podemos aprovechar mais este truco



Comparación datagrama us circuito virtual

Datagrama

- cada paquete en tratado de jorna individual.
 La cabécera de cada uno debe llevor toda la información.
- · Cada paquete puede seguirruta distinta - entrega desordenada
- · Puede haber congestión.
- · Mayor flexibilidad y mayor aprovechamiento de recursos.

Circuito Virtual

- se trata por igual a todos los paquetes con mismo identificados de circuito virtual. cabeceras pequeñas
- · se garantiza que la paquetes llegan ordenados
- · Hay poca (o ningura) congestión, ya que hay un proceso de admisión de conexiones.
 Por contra puede haber bloques
- · El establecimiento de conexión permite controlar mejor el uso ej: fácil de tarificar

3. Servicios

El nivel de red puede ofrecer dos tipos de servicios:

· orientado a la conexión

· circuito virtual

- Sin conexión

Analogía obvia con la entructura de la red · data grana

A perar de la analogía tan clara, pueden combinarse:

ej: Orientado a la conexión sobre estructura datagrama

Datagrama D. H

los nodos se encargan de emularlo

ej. entrega ordenada

ej: Sin conexión sobre entructura circuito virtual.

Puede hacere per en un poco absurdo, ya que disponiendo
de la mayor calidad del circuito virtual ¿ Porque no
aprovecharla con servicio orientado a la conexión?

Además tiene la pequeña pega de que la red sabrá cuando establecer la conexión pero no cuando cerrarla. Esto en importante en las interconexiones de distintas redes de distintos tipos.

4. Funciones del rivel de red

- Encaminamiento

- control de la congestion

- Interconexión de reden

and the particle of the case

- Direccionamiento (identificación de los usuarios)

1 Introducción

· Definición

Hacer parible que un mensaje fragmentado en paqueter llegue a su destino

- menor tiempo posible
- mayor fiabilidad posible

- eliciencia

· Control y Jorwarding

Los nodos ejecutar dor 'algoritmos' simultaneamente 'procesos'

- forwarding: ejecución del encaminamiento

(parar de ma entrada a ma salida) → consulta

- control de encaminamiento: decide a que salida enviar cierta entrada. Decide salidas adecuadas para los distintos destinos - construye/modifica las tablas

· Tablas de encaminamiento

cada pla en un dentino

· como mínimo dos columnas

¿cuando se cre	ar?
· inicialmente?	nosiempre

Destino Salida

A 2
B 1
:

¿ Cuando se modifican? cuando no se cumplar los critérios elegidos

1 pueden ser tablas muy grandes EHay que tener Topos los destinor?!

control de encaminamiento

i Que criterios utilizamos para construir/modificar las tablas?

- · camino más corto (nº saltos)
- · Enlaces más rápidos
- · Nodos menos cargados

Los enlaces de la red tienen asignado

· Camino de menor coste - o un coste

10101

El coste combina los criterios ya mencionados coste = f(nºsaltos, velenlace, carga)

étiemporeal?

No adaptativos

Adaptativos

2. Algoritmos de encaminamiento)

- Inundación

Encamina el paquete por todos los enlaces (salvo por el).

El destino se lo que da (no inunda)

· El destino se lo queda (no inunda)

· en cada nodo hay que mirar la dirección para saberlo

· Garantizamos la entrega por la ruta mejor es sencillo - no hay tablas - no hay protocolos de control

Desventajas:

· Duplicados (control en extremo)

· El trájico crece exponencialmente (buden)

La solución: limitar el tiempo de vida de los paquetes

· un contador en un campo de la cabecera con la hora de entrada. - requiere sincronización en nodos

 contador con el número de saltos
 — el límite en el número de saltos debe ser el diámetro de la red (distancia máxima en saltos sin pasar 2 veces por mismo nodo)

cota diámetro ≤ nº nodos - 1 como máximo

Nota: 1Pv4, aurque no es de desbordamiento, implementa el contador con un byte (256 saltos máximo)

- Aprendizaje retrospectivo

· Aislado: las decisiones se tomas en cada nodo sin tener en cuenta las de otros nodos (no hay intercambios de información de control)

can tablas de encaminamiento son del tipo:

Destino	Salida	Distancia	estimada en el nodo	Tipicamente usado en LAN
A	J 7 en realidad	3 saltos		
	sed una identifical hardwar		the part of	

Inicialmente: nodos desconocen la red

· las tablas están vacias

inundación cuando no sabemor alcanzar el camino (pej.)

se aprende de los paquetes encaminados

Dirección Dirección Numero Origen Destino Saltos

Al recibir un paquete, cada nodo sabe que la dirección origen es alcanzable por el enlace que ha llegado y sabe a que distancia

· si no había entrada en la tabla para esa dirección, la creamos. Si ya estaba en la tabla, pero con mayor distancia, la actualiza

Ventajas:

· el algoritmo converge a las tablas óptimas

no se necesita intercambiar información de control.

· en consistente

Derventaja:

· sólo se aprende a mejor. si cas el mejor enlace no actualizará/ aprenderá distancias mayores

Solución: Reseteur las tablas periodicamente Si T grande - podemos no adaptar

Si T pequeño - podemos no llegar al óptimo

Nota: Tipos de algoritmos

- · aislado: cada nodo decide, sin información de los vecinos · centralizado: un nodo lo decide todo — dY si jalla?! · distribuido
 - se decide en cada nodo
 - -se intercambia información de control (3 protocolos específicos)
 - ejemplos de algoritmo:

- estado del enlace - vector distancia

- vector distancia

· Distribuido y adaptativo

· sólo se informa a los nodos adyacentes y asíncronamente: sólo cuando hay necesidad de tx . Iterativo

Tablas:

- 1 fila/destino

- 1 columna/enlace de salida o vecino

- En cada celda de la matriz: distancia al destino a través del vecino

Notación D^X(Y, Z) ≡ Distancia dende el nodo X hasta Y a través de Z i.e. la tabla del nodo X; fila Y columna Z

$$D^{X}(Y,Z) = c(X,Z) + \min_{W} \{D^{Z}(Y,W)\}$$

$$coste dende$$

$$X hanta Z$$

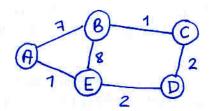
$$dende Z hanta Y$$

$$teniendo en cuenta$$

$$todos sus vecinos W$$

es la que se intercambias los nodos





DE()	A	В	D
A	1	8+6=14	2+3=5
В	1+6=7	8	2+3=5
C	6	9	4
D	4	11	2
•		•	

← parece abrurdo que enviordo a A tuego vueltre, pero esto no es problema ya que el nodo optrará par el canino D, que es mísimo.

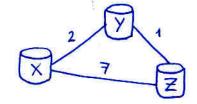
destinos

Las DE con un círculo son el vector distancia del nodo E, y en lo que se comunica a los nodos vecinos.

Pero en realidad él no la puede construir directamente. Hay que seguir un algoritmo iterativo.

← vecinos

Algoritmo paro por paro



Inicialización:

DX	Y Z 2 ∞ ∞ 7	DY	XZ	DE	XY
Y	2 ∞	X	2 ∞ ∞ 1	X	7 00
Z	∞ 7	Z	∞ 1	y	7 00

Ahora cada nodo envia a cada vecino sus distancias mínimas (vector distancia)

Y se entra en el budes:

esperar cambios/mensajes de vecinos recalcular tablas aurisar a los vecinos si hay cambio

sólose avisa cuando combia el MINIMO de una columna

avisor de un cambio de mínimo

DY X Z

X 2 1+7

X 7 1+2

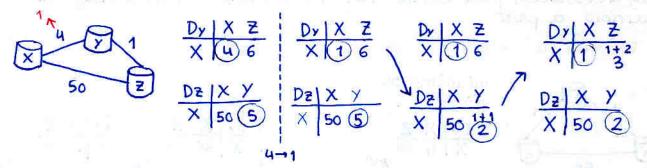
Z 2+7 1

Y 7+2 1

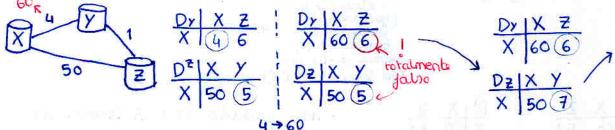
avisar de un cambio de mínimo

este no cambia nada porque no le han lega do cambios relevantes.

Ante un cambio



Si el cambio es a peor, tarda más en propagarse



En ente entado, un paquete a X entraria en un bude

Es una de las desventajas de este algoritmo

Nota: clasificación de algoritmos de encaminamiento.

Estáticos (no adaptativos)

· Inundación

· Encaminamiento entático

Dinámicos (adaptativos)

4 centralización

· Nodo principal, RCC

4 Aislados: cada nodo decide sin info de los demás

· Patata caliente

· Aprendizaje retrospectivo

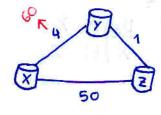
La Distribuidos: cada nodo decide con info de otros

· Vector distancia (info solo de vecinos)

· Estado del enlace (info de toda la red)

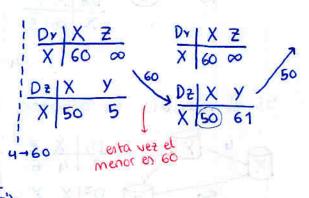
Hay una solución para evitar tantas iteraciones cuando hay un cambio a peor

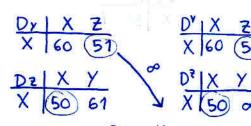
Técnica de retorno envenenado (the llamado horizonte dividido)



inicialmente se usa







· Han parado sólo 3 iteraciones

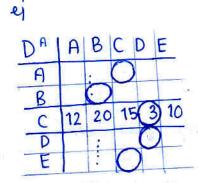
· A veces se llama tambien:

· Horizonte dividido con retorno envenenado

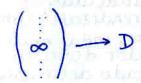
· Inversa envenenado

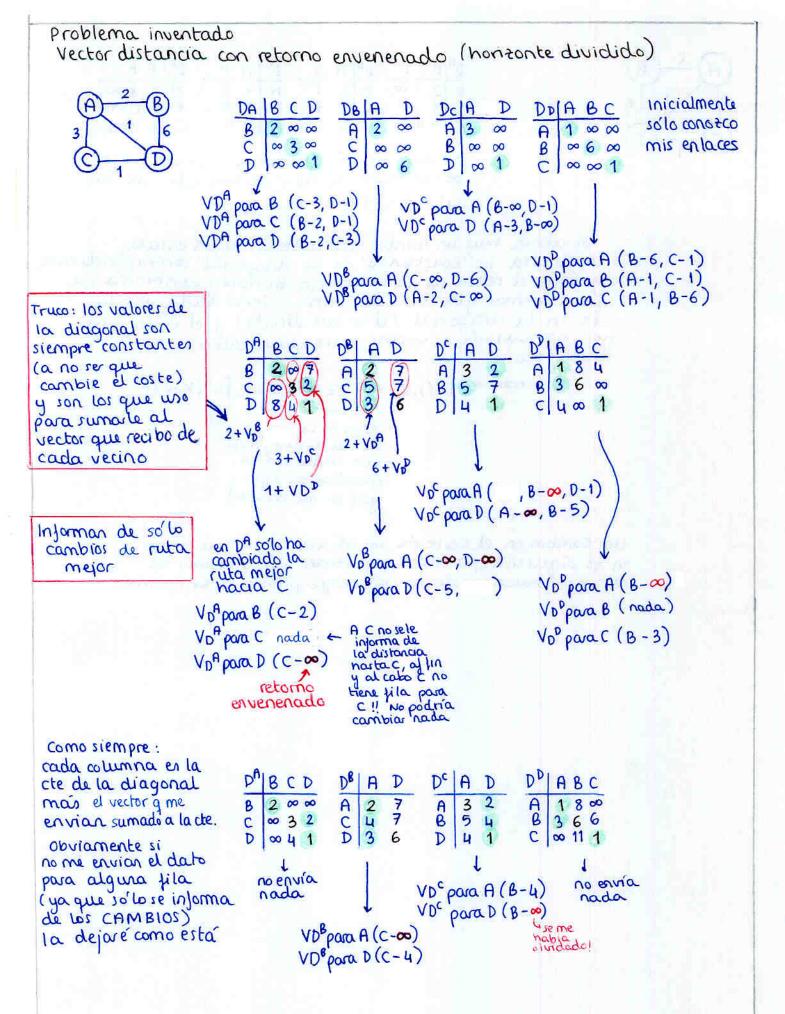
como y debe alanzar X a través de Z, le dice a Z que no lo puede alcanzar · si hay más de dos nodos involucrados, entonces el problema no se resuelve

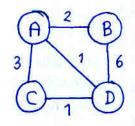
Explicación: cuando informas de la distancia minima hasta un nodo a todos tus vecinos; al vecino por el cual encamines era distancia mínima le engañarás diciendo que tardas ∞



vector dustancia (3) A B C C







DA	BC	D	DB	A	D	Dc	A	D	DP	IABC
B	2 7 ∞ 3	2					3		A	1800
D	∞ u	1	D	2 4 3	6	B			200	3 6 ∞ ∞ 10 1

no hay ninguín cambio en la ruta mejor, por la tanto se han alcanzado ya las tablas optimas

Si ahora hay un cambio del coste en algún enlace, cambiarra la 'constante' de la diagonal correspondiente, y todo el resto de la columna también cambiarra ya que sabemos que una columna viene dada por la cte en la diagonal (el enlace directo) y el vector que nos ha enviado el vecino correspondiente sum a do a dicha cte.

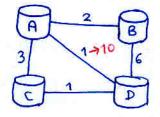
recuerda $D^{x}(y,z) = D^{x}(z,z) + \min_{w} \{D^{z}(y,w)\}$

esta es la
'cte' de la diagonal
que cada nodo
monitoriza (ya
que es su enlace)

un cambio en el coste de un enlace en la que vernor en el siguiente problema, y vernor que gracian al retorno envenenado se converge pronto a la óptimo.

Problema de examen

vector distancia con horizonte dividido con retorno ervenenado



DABCD	DB A D	DE A D	PABC
B 27 00 C 0 32	A 2 7	A 32	A 1 8 00
C \pi 3 (2)	C 4 7 D 3 6	B 5 4 D 4 1	B 3 6 ∞ C ≈ 10 1
D 0 41	V (3) 6	0141	- 10 (I)

vemos que C
no puede
enganar a A
porque a penar de
que su ruta pana
por A, C no losabe,
el sólosabe que ervira a D

aqui A si que engaña a D porque si que se la devuelve DIRECTAMENTE:

"No, no, a mi no me lo parer que te lo voy a devolver"

El coste cambia de 1-10 le sumo el coste a toda la columna

DA IB CID	D ⁸ IAD	DCIAD	DPABC
B 2 7 00 C 00 311	A	AB	A 10(8) ∞ B 12(6) ∞
D 0 4 10 Combios LAVISAR	D	DI	C ∞ 10 1
AVISAR			

Una vez sacamos los vectores que se envian, las tablas se hacen rápido y fácil. VD^A para B: (6-2, C-3, D-4) VD^A para C: (6-2, C-3, **D**-∞) VD^A para D: (6-2, C-3, D-4)

VD para A: (A-8, B-6, C-1) VD para B: (A-00, B-6, C-1) VD para C: (A-8, B-6, C-1)

simplemente se suma el vector distancia con el coste del enlace del que envica dicho vector

No hay cambis en los minimos.

DAIBCD

DB A D

A 2 500

C 257

D 366

elegimos este porq este directo

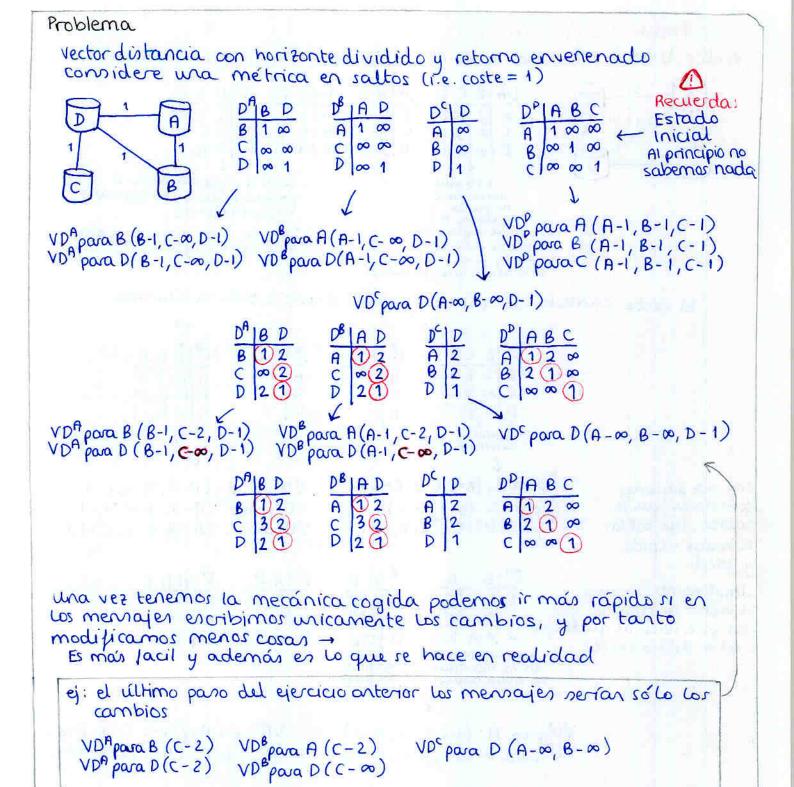
D° A D D° A B C A 3 9 A 10 8 ∞ B 5 7 B 12 6 ∞ D ∞ 1 C 13 10 1

VD^B para A: (A-2, C-∞, D-6) VD^B para D: (A-2, C-5, D-6)

VD^c para A: (A-3, B-∞, D-1) VD^c para D: (A-3, B-5, D-1)

D^C | A D D^D | A B C A 10 8 W B 12 6 6 D C 13 10 1

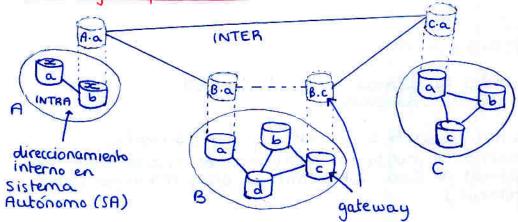
VD^D para A: (A-4, B-6, C-1) VD^D para B: (A-4, B-6, C-1) VD^D para C: (A-∞, B-6, C-1)



3. Forwarding (retransmisión) consulta de tablas.

3.1 Encaminamiento en redes grandes

· Redes jerarquizadas



Problemas con redes reales:

- · gran número de nodos
- · autonomía administrativa

Solución:

- agrupar en sistemas autonomos SA: Nodos dentro de SA ejecutas mismo algoritmo (Intra-SA)
- · conectar SA con nodos gatemay (pasarela) Protocolo de encaminamiento Inter-SA

ejemplo: esquema de arriba Tabla de encaminamiento de B.d suponiendo coster = 1

B.d	<u> </u>		B.c	landar.
a	al	ſ	a.	d
b	b nodes en - 1	1	b	b
C	C) 34 3H	L	d	d
A	a Inodesa -1	ſ	A	d
C	C		C	C.a

ejempla: 720 nodos

· sin jerarquia: 719 entradar en tabla

· 2 riveles

24 reg : 23 + 29 = 52

30 nodos/rea

....

Nota: Con N nodos, el número de niveles éptimo para minimizar tablas es en N niveles → tablas con e la N entradas

Ventajas:

· Reducción tablas

· Flexibilidad reconfiguración

· facilità crecimiento

perventajas:

. mayor tráfico sobre gateways . Algunos nodos pueden seguir

rutar menos optimas

· Encaminamiento por dejecto

En las tablas aparece entrada dijault. si no tengo el destino que busco en mis tablas, lo envio por default

4. <u>L'Encaminamiento</u> a mais de un destino

Broadcast: a todos los demás nodos de la red No requiere dirección

multicart: enviar paquete a un subconjunto de nodos suponemos la grupos ya gentionados (no en Jacil, en Internet se usa IGMP Internet Group Management Protocol)

Técnicas de difusión

1. unidifusión uno a uno a los destinos: trivial

2. multidestino: mando a unos cuantos y esos mandas a los que quedas

-Para broadcast

3 · Inundación: se envia paquete a todos los nodos

4. Inundación controlada = spanning tree adaptativo o dinámico

5 spanning tree:

- Para multicant

5 · spanning tree (arboi de grupo compartido)

4 spanning tree adaptativo o dinamico

1. Unidifusión de uno a todos los destinatarios

· sencillo de implementar

· Ineficacia en el uno de enlaces

2 . Multidestino:

· se mete en el paquete la lista de destinos En el Nopo te la que dan si en parati y la reenvian a algunos que

· Réquiere formato especial de paquetes

3 . Inundación:

· Nodo envia por todos enlaces menos el que llego.

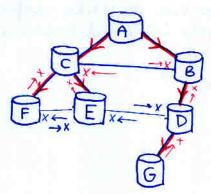
· muy sencillo y rapido

· Ineficiente, duplicaidos, bucles

· inundación controlada/spanning Tree adaptativo o dinámico

RPF (Reverse Path Forwarding) & RPB (Reverse Path Broadcast) también lamado Spanning Tree adaptativo o dinámico

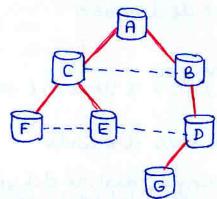
un nodo retransmite el paquete sólo si le llegó por el enlace que está en el camino de mínimo coste hacia el nado origen



- · mantiene la ventaja de direccionar a un isla destino
- · Aún llega mas de una copia del paquete a cada nodo

5 . Spanning Tree

cada nodo debería recibir sólo una copia del paquete Hacemos un árbol como:



- · contiene todos los nodos
- · contiene subconjunto de los enlaces sin budes y todo conectado
 - · Primero re construye el árbol: sirve para todos los nodos
 - Los nodos ervian sus paquetes pertenecen al arbol.

ventajon:

- elimina paqueter redundantes y no hay budes cada nodo solo debe saber en laces que pertenecen al a bol

- mismo árbol para cualquier nodo

perventajar:

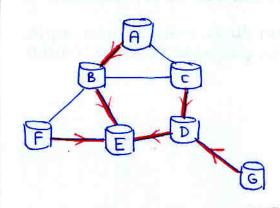
- necesario determinar el arbol previamente
- si falla un enlace fallarán futuras difusiones
- pueden haber paquetes que no reguirán rutas más cortas

Algoritmo de creación del árbol.

· Barado en nodo central

cada nodo envía un mensaje al nodo central; el mensaje se retransmite hasta llegar al nodo central o a un nodo que ya pertenece alárbol.

- El camino que el mensaje ha seguido define la rama del árbol entre el nodo que inició el mensaje y el centro



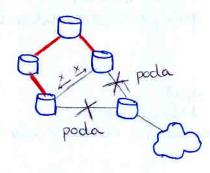
Para multicart

· Spanning tree Igual pero el árbol so lo incluye al grupo de dijusión

Spannig tree adaptativo o dinâmico / difusión modificado
El arbol se genera seguin se envia el mensaje.
El nodo repite el paquete que le llega sólo si le llega del camino más corbo al origen.

Esto significa que el mensaje llegaría a todo el mundo

Mejora: poda si un nodo no lleva a ningún destino del grupo, envía un mensaje de poda (poda la rama del árbol) para que no vuelvar a enviarle.

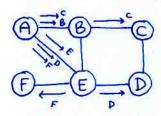


Problema de difusión

calcular la eficiencia

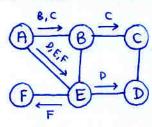
wardo los siguientes algoritmos:

a) Envio de un paquete a cada destino



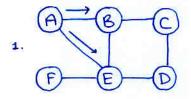
$$E_1 = \frac{5}{8}$$

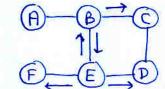
b) multidestino

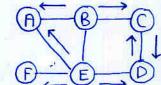


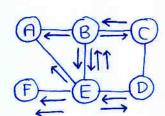
El coste es que necesitamos modificaciones en los algoritmos para soportar varias direcciones.

c) Inundación (diametro = 5)

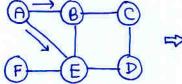


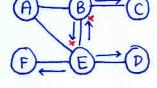


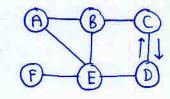




d) Spanning-tree adaptativo

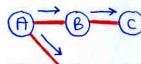






e) spanning tree

vemos que forma tendría el árbol utilizando nodo central (todos envias mensaje)

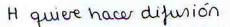


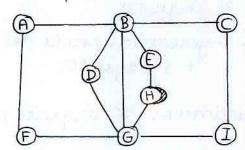
Junio 2004

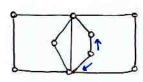
Problema 6

- · Inundación 4 saltos
- · Span. Tree D
- · Span Tree Dinámico

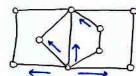
· Inundación 4 saltos



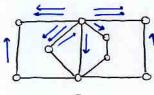


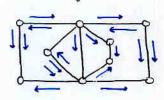




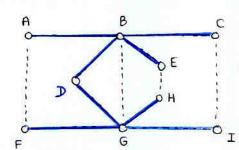


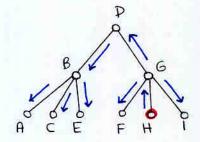






. Span. Tree - (Todos enviar mensaje a D para generar el tree)



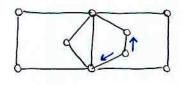


ura vez hecho el árbol, el broadcant puede hacere dende cualquier node, no sólo dende el órigen' del árbol

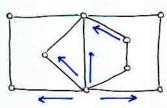
una vez generado el tree, cuantos paqueter se generan al hacer H difunión

ecuerda: cada nodo envia loque le llega por todos sus enlaces excepto por el que le llega siempre y cuando le llegue pordomino más corto hacia H (emisor).

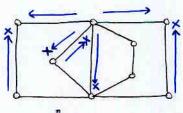
Rechaza los que no le llegan por el camino más corto

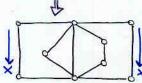












comparación:

· Inundación: 35 paquetes

· spanning tree: -generación previa del aírbol + 8 paquetes

· Spanning Tree dinámico: 16 paquetes

Tema L. control de la congestión

11. Introducción

El problema de la congestión

paqueter entregados maxima capacidad deseable congestion > paqueter enviados

- · paqueter derbordar noda en capacidad de almacenamiento y velocidad a la que debe cursor
- vecinos Uenar colar de salida hacia el nodo congestionado y se va extendiendo congentión

Causas:

- · capacidad almacenamiento

· velocidad procesadores · capacidad de enlaces

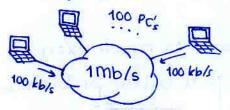
insuficiente

Dificil solución:

- . Aumentar recursos no lo elimina, sólo lo retrasa
- · cada vez mas usuarios con demandas mas diversas
- · Picos de trájico > no banta dimensionar para trájico medio

control de congestión:

Tiene en cuenta toda la red (g sea capaz de cursar el trafico)



Control de jujo

Tiene en cuenta tráfico punto a (au el tx no desborde al rx)



Tecnicas de control de la congestion

- · Preventivas o de cido abierto Decisiones a priori para evitar llegara la congestión
- · Curativas o de ciclo cerrado se basa en una realimentación de lo que sucede en la red

2. Técnicas preventivas o de ciclo abierto

2.1 Diseño y configuración a varios niveles

- · Enlace de datos :
 - · timeouts
 - · tamaño de ventanas
- · go-back-n o retransmisión selectiva
- · reconocimiento (piggybacking frente a tramas específicas)

- · Nivel de red:
 - · circuito virtual o datagrama
 - · algoritmo de encaminamiento
 - · tiempo de vida de los paquetes
- · Nivel de trans porte:
 - mismos jactores que el rivel de enlace
 - · timeout man dificil de optimizar

2.2. Control de admisión

- · originariamente pensado para redes de circuito virtual
- · control de admisión básico: si se detecta congentión no se admiten más conexiones
- CAC (control de Admissión a la Conexión)
 Nodo origen solicita establecimiento, y lesigue una
 negociación (origen envia parámetros del tráfico que
 necesita y CAC calcula recusos necesarios)
 se acepta o no la conexión si se podrá satisfacer la (auality
 of service) QoS

2.3 Asignación de recursos

· Asignación de memoria en la nodas previa a la transmisión

Hay que asignar sabiamente la memoria para evitar problemas Tipos asignación:

- Fija: repartir buffer entre lar enlaces 2000 ej → podria blaquearse un enlace habienda memoria en otros

- Dinámica :

La un enlace podria acaparar la memoria

- Dinámica con límite: M & N mem total

max buffer para nº enlaces

un enlace (límite)

M.

ej: 9 bullers 3 enlaces

· Buffers exclusivos: Siempre se garantiza memoria para un paquete nuevo que sólo se atendera si ueva información que permite liberar otros buffers.

24 Adecuación del tráfico

Evitar el tráfico a rajagas (burst) que generar algunas aplicaciones transformándolo en un flujo más constante que facilite el control de la carga en la red.

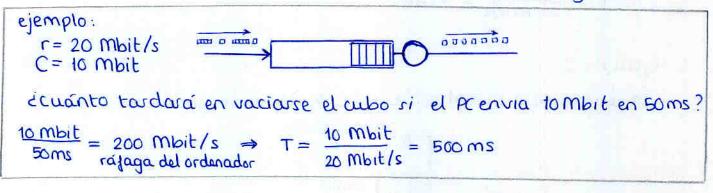
· Cubo con gotera (leaky bucket)

- se almacenan los paquetes del usuario y se envian a un flujo regular.

r: (b/s) caudal de salida

C: (b) capacidad del buffer

si la memoria re llena → o se rechazan más paquetes → o se envian marcados de 'menor prioridad' = eliminan si hay congestión.



· Cubo con permisos (token bucket)

Permite rájagas pero con ciertas limitaciones Logra limitar el flujo MEDIO. (average rate)

- · se generar permisos regularmente: r (permisos/s = bit/s)
 - · Capacidad máxima de permisos igual a la capacidad del buyer C
- · Los permisos se utilizar para enviar datos a un caudal mayor M (bit/s)
- · cuando se agotar los permisos funciona como el cubo con gotera, al caudal menor r(bit/s).

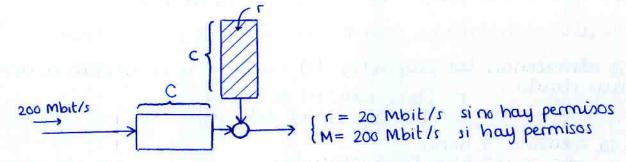
 En ese caso no se van generando permisos mientras se envia a r.

Una forma más lógica de ver esto último seria que cuando se agotar los permisos no re pueden erviar más datos, pero como constantemente se están generando permisos a una tasa r(bit/s) entonces los datos pueden ir saliendo a la tasa r(bit/s) utilizando esos permisos según se crean

ejemplo 1.

r = 20 Mbit/s C = 10 Mbit M = 200 Mbit

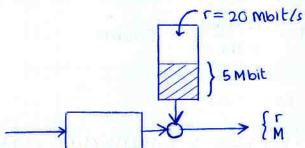
PC envia 10 Mbit en 50 ms Inicialmente lleno de permisos



Los 10 Mbit saldrán directamente a M. $T = \frac{10 \text{ Mbit}}{200 \text{ Mbit/s}} = 50 \text{ ms}$

ejemplo 2.

¿ aux ocurre si inicialmente está 1/2 lleno de permisos?



cuidado, podría pensarse que se envia la mitad a M y la otra mitad a r; pero hay que tener en cuenta que mientras los permisos no estén vacios, van llegando más a r bit/s. (nota: dejan de llegar permisos una vez se han vaciado todos; si no te convence les el ultimo parrajo de la cara anterior)

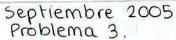
¿cuánto tarda en vaciorse los permisos?

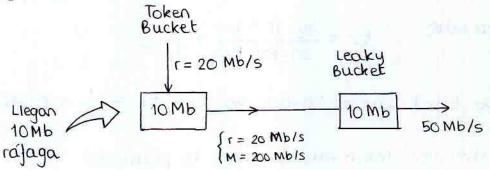
despejando; tm = 1/36 s

En ese tiempo hemos transmitido M. tm = 50 mbit

Al llegar tm, requeda vacía la reserva de permisos, y simplemente se transmite lo que queda a la tasa menor r (igual a la tasa de generación de permisos)

$$tr = \frac{10 \text{ Mb/t} - \frac{50}{9} \text{ Mb/t}}{20 \text{ Mb/t}/c} = \frac{2}{9} \text{ s} \implies T = tm + tr = 250 \text{ ms}$$





- a) Token bucket inicialmente vacio de permisos
 - Del token bucket sale a 20 Mb/s, limitado por la generación de permisos
 - · El Leaky bucket no tiene ejecto. Llega a 20 Mb/s y sale a 20 Mb/s

$$E = \frac{10 \cdot 10^6}{20 \cdot 10^6} = 0.5 s$$

b) Token bucket medio ueno de permisos (5Mb de permisos)

Cuidado: A 200 Mbls von a salir un poco mais de SMb ya que mientras sales se estas generando permisos.

de permisos es cero

se despeja:
$$t_0 = \frac{1}{36} s$$

Ahora al leaky bucket le llegara un rato a 200 Mb/s y él lo sacará a 50 Mb/s y hugo seguiran llegando a 20 Mb/s

$$200 \cdot 10^{6} \cdot t_{0} + 20 \cdot 10^{6} (t_{1} - t_{0}) - 50 \cdot 10^{6} \cdot t_{1} = 0$$

$$200 \cdot 10^{6} \cdot \frac{1}{36} + 20 \cdot 10^{6} (t_{1} - \frac{1}{36}) - 50 \cdot 10^{6} \cdot t_{1} = 0$$
bits que bits que llegar bits que saler a 50 Mb/s

En ti es cuardo el cubo queda vacio; es decir cuardo dejan de salir a 50 Mbls

$$t_1 = \frac{1}{6}s \longrightarrow 50.10^6 \cdot \frac{1}{6} = \frac{25}{3} \text{ Mb}$$

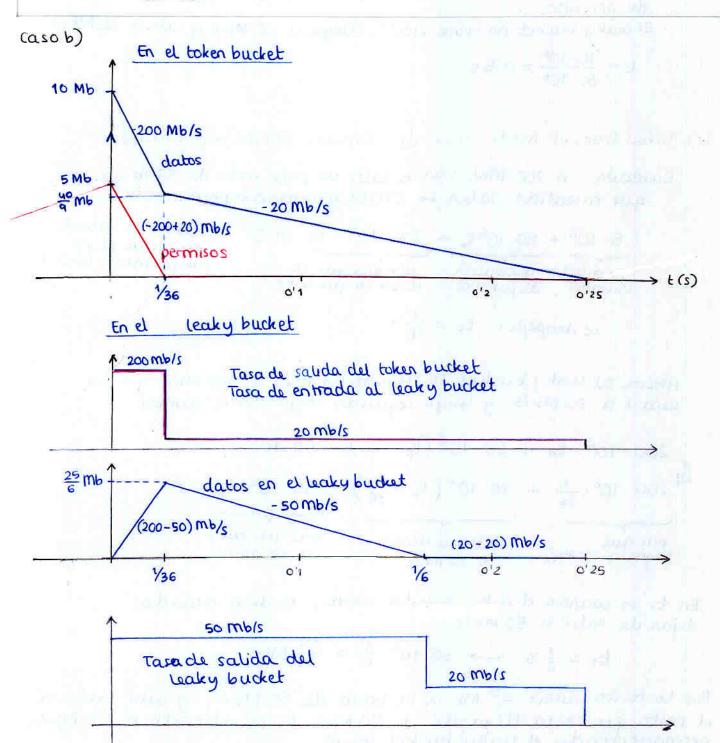
Por le tanto salen $\frac{25}{3}$ Mb a la tasa de 50 Mb/s, y aux jaltara el resto que esta llégando a 20 Mb/s e ira saliendo a 20 Mb/s, permaneciendo el liáky bucket vacio. IV-2.2

A 20 Mb/s quedan por salir
$$10 \cdot 10^6 - \frac{25}{3} \cdot 10^6 = \frac{5}{3} \cdot 10^6$$

Tardan en salir $t_2 = \frac{5/3 \cdot 10^6 \text{ b}}{20 \cdot 10^6 \text{ b/s}} = \frac{1}{12} \text{ s}$

El tiempo total que se tarda en $t_1 + t_2 = \frac{1}{4} = 0'25 s$

c) Inicialmente Token bucket Ueno de permisos salen Los 10 Mb a 200 Mb/s y el leaky bucket Los saca a 50 Mb/s $t = \frac{10 \cdot 10^6}{50 \cdot 10^6} = 0'2 \text{ s}$



3. Técnicas curativas o de ciclo cerrado

Se basar en una realimentación de lo que ocurre en la red. Inicia acciones para:

· Cambiar la tendencia de acercamiento a la congentión

· salir de la congentión

Tres jases:

- Monitorización del estado de la red Periódicamente se monitorizar distintos parámetros (paquetes descartados, tamaño de colas, número de retrassmisiónes...)
- · Envio de información

Donde se detecta o información porde se puede hacer algo predice la congestión para evitarla

- · reservar espacio en cada paquete (ej: warning bit)
- · enviar paquetes periodicamente preguntando · enviar paquetes al nodo origen.
- · Ajuste de medidas correctoras

3.1 Paquetes de restricción (Choke packets)

· Se muestrea periódicamente (frecuencia de muestreo) cada uno de los enlaces de un nodo.

En dicho muestreo se estima U (factor de utilización del enlace) haciendo:

Unew = a. Wold + (1-a). j

U € [0,1]: jactor de utilización

a ∈ [0,1]: jactor de olvido

1 = {0 enlace libre } en el momento de muentreo

· Si Unew > Unmbral
se envía un paquete de
restricción al origen del paquete
que ha disparado la alarma

coincidencias con ese instante de muestres pueden dar predicciones falsas

W-3

· Llega paquete de restricción al nodo (y no hay ningún T2 activo)

- Reduce la tasa de transmisión en un x%

→ Activa temporizador T2 durante el cual ignorará nuevos choke packets (compensar retardo de propagación)

→ Activa temporizador T1>T2, si vence T1 sin haber recibido nuevos choke packets (sin contar los recibidos duante T2), recupera el flujo original.

ejemplo de temporizadores: CP3 CP4 CP1 CP2 T2 > - 50% 50% + 50% ignora ignora - 50% 50% 25% 50% 100% Problema: . Red conmutación paquetes tipo datagrama vel tx = 10 Mbit/s long paquete = 10 kbit 50 pag/s · control de congestión mediante paquetes de restricción. frec evaluación u = 100 veces/s $\dot{a} = 0.5$ Sabiendo que en To se está recibiendo paquete y se está evaluando U, siendo lloid = 0'2, y sabiendo que en To + 60 ms se empieran a enviar paquetes de restricción; calcular UH. calculamos: - duración paquete 10kbit/s = 1 ms - muestres U cada $\frac{1}{100}$ s = 10 Ms · se envia paquete cada 20 ms Unew = Uold·a + f. (1-a) 1ms T3 10 ms L Unew > Uth 20 ms u = 0'2.0'5 +0'5 u = 0'325.0'5 + 0'5u=03.05+05 U=0'33125.0'5 +0'5 = 0'6 = 0'6625 = 0'65 = 0'665625 u=0'6.0'5+0 u=0'65.0'5 u = 0'6625.0'5 = 0'3 = 0'325 = 0'33125 Por tanto 0'6625 < Uth & 0'665625

mejora: Hop by hop choke packets

Desde que hay congestión y se envia el choke packet al emisor hasta que este le llega hay un intervalo de congestión en el cual se estan perdiendo paquetes.

Con la mejora hop-by-hop choke packets se alivia el problema haciendo que la reducción de tasa se haga en todos los nodos por los cuales pase el choke packet (ello implica que tengas cierta capacidad de almacenamiento)

3.2 Descarte de paquetes (bad shedding)

cuando los nodos no pueden manejar los paquetes que reciben simplemente los descartan.

Descarte selectivo:

· según aplicación:

- old is better than new (4: tx picheros)

- new is better than old (ej: videoconferencia)

· según prioridad del paquete se descartar primero los paquetes de menor prioridad (recuerda, así se enviabar los paquetes que sobre pasabar la maxima capacidad del leaking bucket, con menor prioridad) the state of the s

Tema 5. Interconexión de redes

1. Introducción Conceptos y problemática

1.1 Introducción

unica red homogenea mismos protocolos Hasta ahora

En realidad hay muchas redes distintas consolidadas

PC's : TCP/IP

Empresas : SNA de IBM

Comparian Telecom: reden ATM

LANS: Novell a Apple Talk

WLAN

Al boyor coste de PC's y reder, hay más variedad.

1.2. d'En que se diferencian las reder?

Nivel físico: - medio tx

- tecnicas modulación

Nivel enlace: - formato de tramas

Nivel red: - servicio (orientado o no a la conexión)

- protocolos (ip, sNA,...)

- direccionamiento: (plano (802), jerárquico (IP)) - multidentino (permitido o no, broadcanto no)

- tamaño paquetes (cada red con su maximo)

- calidad 'de 'servicio (Qos) soportada

- Errores (servicio fiable o no, entrega o no) - Control de Juyo (ventana deslizante, regular vel tx)

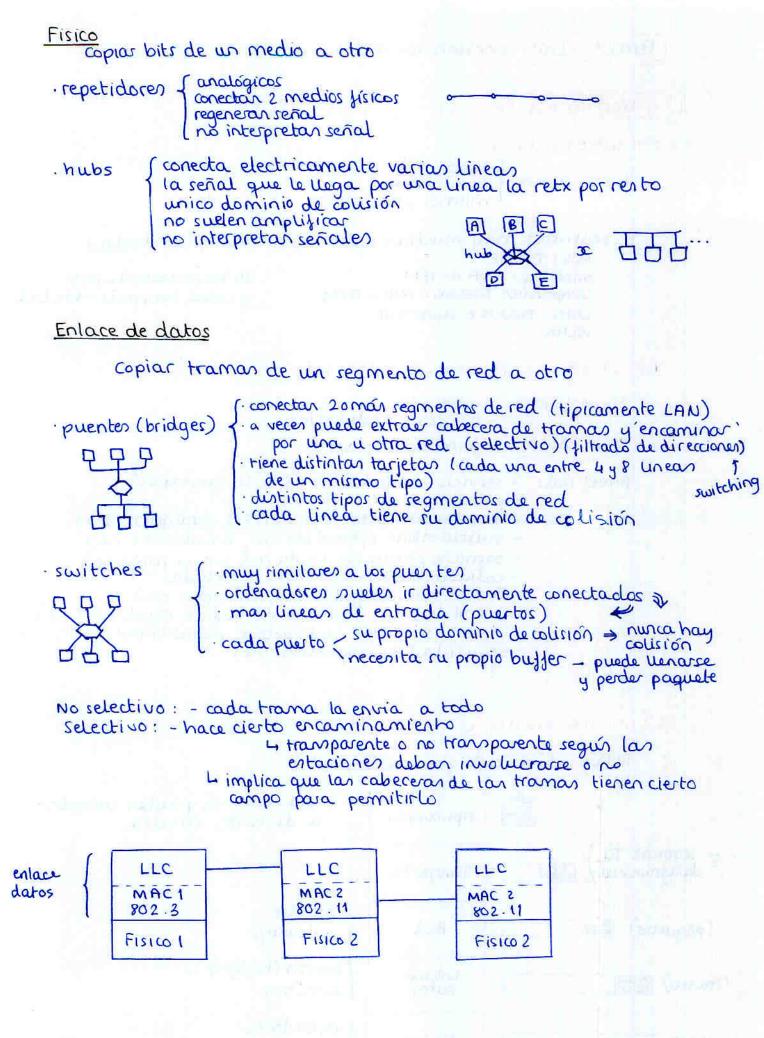
- control congestión (cubo gotera, paquet en restricción,...)

- Seguridad (encriptación o no)

13 d'Como pueden conectarse?

Relays: dispositivos que conectar redes

A REAL PROPERTY OF THE PARTY OF	والمشارع والأرابية	
User Data	Aplicación	Las redes se puedes conectar a distintos niveles.
(segmento TCP) tcp datagrama UDP) meader	Transporte	
(paquetes) Market	Red	{ routers gateways
(tramas) France	Enlace Datos	{puinter (bridger) switcher
(sits)	Fisico	{ repetidoren }
		- T



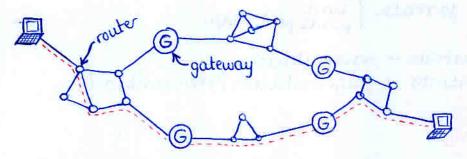
Routers { dos o mas redes iguales paquete - extrae cabecera y encamina no hace conversiones de paquetes

Pararelas { · router multiprotocolo (Gateways) { · hace conversiones y/o encapsulado

A partir de ahora nos Hjamos en el nivel de red

2. Concatenación de redes

2.1 Orientada a la conexión



se crea un único camino para los paquetes

Ventajan:

- reverva buffers

- garantiza entrega en orden

- cabecerar más cortas

- elimina duplicados

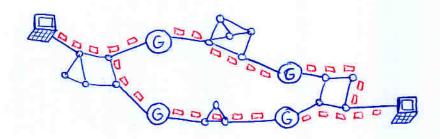
Inconvenientes:

- requiere reservor espacio para cada conexión

- vulnerable ante fallos nados

practicamente imposible si una red intermedia estipo datagrama (no garantiza entrega ordenada, etc...)

2.2. No orientada a la conexión



Ventajas:

- mayor velocidad tx (por usar mas router)

-mas robusto frente a jallos de nodos

Inconvenientes:

- no garantiza entrega en orden

- mas propenso a congestión

- cabeceran + largan

2.3 Probleman

· Formato distinto

· Tamaño distinto

solución:

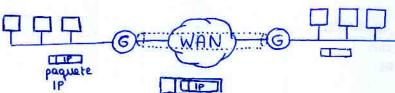
- conversión formatos (complicado - puede perder info

· formato distinto - encaprulación

· tanaño distinto - jragmentación / reensamblado

Tunnelling)

· Reder de origen y destino iguales · conectadas tipicamente por red tipo datagrama (usualmente WAN)



Pone el paquete IP integro en la carga del formato que sea) lla WAN con dirección destino el otro gateway

virtualmente hay un enlace directo entre ambas redes

4. Fragmentación)

una red tiene un tamaño máximo de paquete (incluso mínimo)

segun:

· hardware

· sist. operativo · protocolos

· estándares

· citerios de diseño

Para poder parar de una red a otra

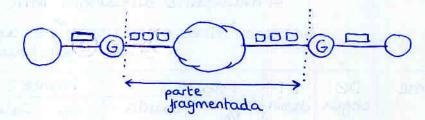
· dividir en fragmentos

· duplicar cabecera (cada paquete requiere cabecera)

puede requerir añadir/modificar (control/relleño)

Reensamblado:

· Transparente

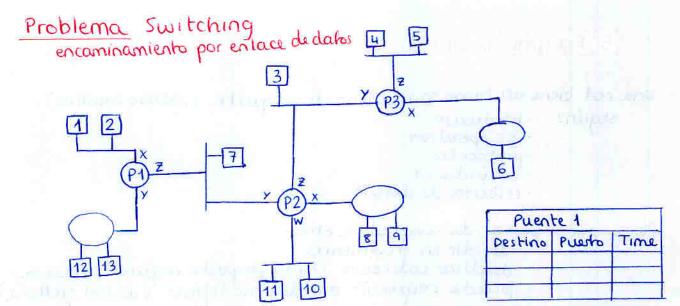


· No transparente



· Es el usuaro el que debe reensamblar los paquetes

· No limita la ruta que pueder seguir los paquetes



D = hosts

(P = puenter => Estamos a nivel de enlace de datos

sólo 3 entradas. va borrando la más vieja

hacemes "direccionamiento" por aprendizaje retrospectivo

Time	DO	DD	Puent		Puer	nte 2	Pu	ente 3
	ongen	dentin	¿Reenvia?	satida	S/N	Salida	SIN	Salida
1 2	1 2	9 12	5	- Y, Z Z, Y	5 5	W, X, Z W, X, Z	S	E,X E,X
		io unali a	or good so		. را <i>ندا</i> ب	المساوعي في	agy rab	4.9

difunde y aprende

	Puente	1
Destino	Puerto	Time
1	X	1
2	X	2

Pu	ante 2	
Destino	Puerto	Time
1	У	1
2	Y	2

Puer	ite 3	
Destino	Puerto	Time
1	Y	1
2	Y	2

Es muy metódico

1. Buscar destino en tabla
si la tenemos, enviar por ese puerto - nos llega, lo descartames
si no la tenemos, enviar por todas

2. Actualizar tablar (siempre)

· sabemos que el origen se alcanza por el puerto de entrada;

si ya estaba: actualizamos time

si no estaba: sobreescribimos la tabla (sobre la entrada de time mas viejo)

Introducción. Internet

Antecedentes

ARPANET 1969 - red militar para resistir un ataque Red de conmutación de paquetes no orientada a conexión

2. IPV4

2.1 Introducción

Filosofia arquitectura DARPA:
Red constituida por multitud de redes

· Interconectadas por routers

U.S. backbone

European backbone

National Network

PPP LAN

Niveles:

Aplicación	de Host
Transporte	OF HOSE
Internet	niveles
Transporte lísico o acceso a la red	de IMP

Protocolo IP:

- · sin conexión and the managing for an examinating activation of managing
- · datagrama
- · modo transmisión best-effort

version	Header	Type of Service	T	otal Length
lo	dentifica	rfiou	DF MF	Fragment Offset
Time to live Protocol		Head	er Checksum	
	Sou	uce IP address	entar 2	U.S. Raddesin
	Destina	tion IP address		

Version: version del protocolo IP i.e. 4 si es IPV4

Tamaño cabecera: en palabras de 32 bits [5, 24-1=15]

Tipo servicio:

| D T R X X no están en uso
| prioridad delay reliability | throughput

Longitud total: (de cabecera + datos) en bytes [20, 216-1 = 64k]

control de tragmentación:

- Identificación: identidad única de cada tragmento

- DF: Don't Fragment: a 1 si no se debe fragmentor; les fragmentes le llevan a 1 (i.e. 1850 le puede fragmentaire 1 vez)

- MF: More Fragments: a @ si en el último

- Offset de Fragmento: la posición del fragmento en el paquete original (contado en bloques de 8 bytes)

Tiempo de vida: Inicialmente a 255. Antiguamente segundos!, ahora saltos?

Protocolo: El protocolo que va encapsulado en DATA (RFC 1700) ej 6=TCP, 17=UDP

Checksum de cabecera: coger bloquer 16 bits, hacer Ca1, sumar, hacer Ca1 se recomputa en cada salto (ya que cambia Tiempo de vida)

Dirección IP origen Dirección IP destino

2.3 Direccionamiento y subredes

· una dirección IP por cada interfaz · 32 bits - 4 grupos de 8 bits

ver RFC 1166

Tiene 2 parter

Net-ID (asignado por organismos) Host - 10

clase A

RED (7 bits) HOST (24 bits)

Margen de 5 1.0.0.0 directiones A 1126, 155, 155, 155

Clase B

RED (14 bits) 1 0

HOST (16 bits)

128.0.0.0 191, 255, 255, 255

Clase C

RED (21 bits)

HOST (8 bits)

192.0.0.0 223.255,255,255

Clare D Multicast 1110

1111 - uso futuro

Direcciones reservadas

Como sirven para cualquier clase A,B,C la hago genérica mando la nomenclatura red. host - ej. red. 0 sería (red. 0.0.0 si clane A red1. red2. 0. 0 si clane B

red a ceros:

O. host: indica ESTA red (ej: al inicializar PC)

todo a ceros:

: indica ESTE host

todo a unos:

255.255.255.255: (todo unos) broadcast en mi red

red. 255: broadcast en red indicada host a wnos:

127. host: loopback: se trata paquete como entrante

127. x.x.x 01111111. x.x.x

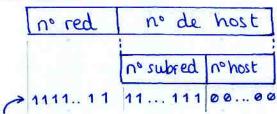
En resumen: bits 0 = ESTE

bits 1 = TODOS

Problema:

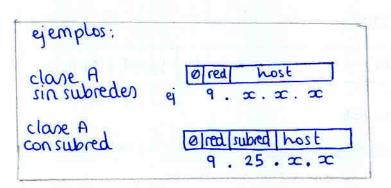
Es absurdo si queremos hacer varian reden pequeñan (ej 5 hosts) ya que en el peor cano (dane A) malgantamos los 16 Mhosts disponibles. Se acabarian enseguida las direcciones de reden

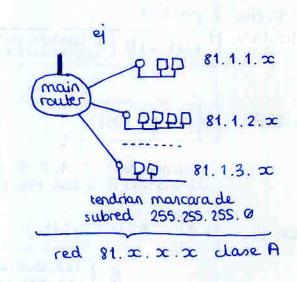




con la máscara de subred distinguimos entre los bits de red/subred y los . del host.

Todas las subredes de usa musma red deben tener misma májcara





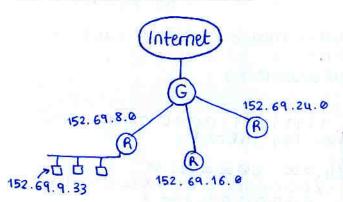
Aun ari puede ser ineficiente para redes pequeñas (255 hosts son muchos bits malgartados para LANs de 3 o 4 PC's)

solución:

- direccioner de red con longitud variable RFC 1519
- complica mucho el encaminamiento

Mascara de Subred para encaminar

Para saber a donde encaminar un paquete, necesitamos saber la subred de la dirección. Para ella hacemos la AND bit a bit con la máscara de subred.



Llega paquete para 152.69.9.33

152.69.9.33

AND 255.255.248.0

152.69.8.0 — dirección de la subred a la que direccionar

en bils: 152.69.00001001.00100001 AND 255.255.11111000.00000000 152.69.00001000.00000000

Por ero es importante que todas las subredes tengas la misma máscara; excepto...

CIDA. Subredes con distinta mascara

RFC 1518 - 1519

· complica el encaminamiento.

· Hay que hacer la AND con todar las máxaras y ver que resultado coincide con una subred. Si coinciden varios hay que que darze con la máxara de más unos o visto de otro modo, aplicar todar las máxaras en order decreciente según nº de unos y quedarse con la primera coincidencia

· Permite hacer variar subdivisiones

Problema Junio - Subredes

Disponemos de la dirección de red 152.69.0.0 empieza por 10 → clane B Queremos segmentos con ≤ 2000 hosts/segmento

Elección de máscara de subred:

red clane B subred nost

Thit = 32 11 bits → 2048 > 2000

excluyendo los canos reservados (todo ceror y todo unas)

tenemos: 30 posibles subredes con 2046 hosts cada una

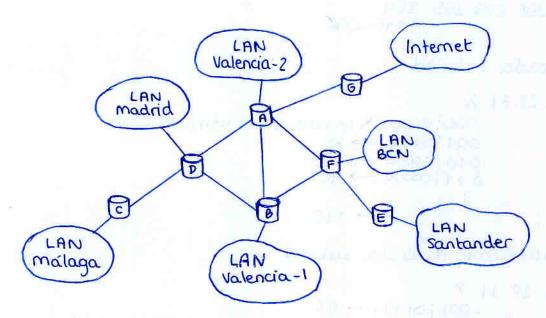
Dirección de las subredes:

152.69. xxxxx0000.0 $0000000000 \rightarrow revervada$ $000010000 \rightarrow 152.69.8.0$ $00010000 \rightarrow 152.69.16.0$ $000110000 \rightarrow 152.69.24.0$ $11110000 \rightarrow revervada$ $111110000 \rightarrow revervada$

```
aueremos
Tenemos dirección IP 156, 134.0.0
                                        10 subreden de 250 hosts
                                                   de 1000 hosts
                                        12
                                                   de 8000 hosts
Usaremos distintar mascaras de
subred. Emperaremos à asignar desde mayor à menor numero
de bits de subred. Habra que tener MUCHO CUIDADO CON NO
SOLAPAR las reder posterioires a las anteriores
· 10 subreder de 250 hosts
                            Asignamos las subredes
 250 - requieren mínimo
                             156. 134, xxxxxxxxxx. 0
        8 bits
                                     Como 156.134.0.0 es de
clase B, disponemos de 16
 bits i.e. - 8 bits rubred
                                       0001000
 mascara de subred sera
                                           01001-
                                     00001010
 255. 255. 255. 0 / 24
12 subredes de 1000 hosts
                                Asignamos las subredes
 1000 hosts { 10 bits host bits subred
                             156. 134. xxxxxxx00.0
                                     X 0 0 0 0 0 0 0 0 0 → X reservada
 maiscara de subred será
                                     XO O O O O 1 00 - 4(5,6,7) Y
                                     X00001000 - 8(9,10,11) USAPAS
                                      00001100-12)+4
 255. 255. 11111100. 0/22
                                             10000 - 162+4
 como ver hay que tener cuidado
                                                               12 subredes
 de no solaporse con las ya uradas
                                                       - 24
                                              0 1
                                                       - 52
 5 subredes de 8000 hosts
 8000 hosts { 12 bits host 4 bits rubred
                               156. 13u_{-1} \propto x \propto x_{-1}0000. 0
                                        0 0 0 0 0 0000 - 0 XIEZEN
                                                0000 - 16 X YA
                                        0001
 máscara de subred será
                                        0010
                                                             USADAS
                                        0011
                                                0000 - 48x]
 255.255.11110000.0 /19
                                        0 1 0 0 0000 - 64
                                        0101
                                                      - 80
                                                             (5 subredes
                                                      - 96
                                        0110
                                        0 1 1 1
                                                       -112
¿ aux ocurres i ahora llega un
                                                      → 128
                                       1000
  paquete para 156.134.57.120
se hace la AND con todas las máscaras y se coge la que coincida
con mayor tamaño de márcara (mai uños = menos hostr)
                        124 → 156. 134. 57. 0 → no coincide con subred
                        122 -> 156. 134. 56. 0 -> coincide -> tomamos
                  AND
                        /19 -> 156.134.48.0 - coincide
      0011 1000
```

Problema subredes usando CIDR

Problema 1



- Se asigna dirección de clase C 194.28.37.0

· Subred para cada LAN: 6 subreden /25 direccionen IP

· Subred para cada enlace: 8 subreden / 2 direccionen IP entre dos routes

Para los enlaces: (emperar siempro por la subred con mais bits de red)

2 dir IP { 1 bits de host entanan los reservados o para la sub red 2 bits de host 6 bits subred

• Marcara: /30 = 255.255.255.252

· Direcciones subredes:

Broadcast:

194. 28. 37. \(\infty \)

194. 28. 37. \(\infty \)

000000 00 \(\to \)

000001 00 \(\to \)

000010 00 \(\to \)

000010 11 \(\to \)

194. 28. 37. \(\infty \)

000001 11 \(\to \)

194. 28. 37. \(\infty \)

000001 11 \(\to \)

194. 28. 37. \(\infty \)

000001 11 \(\to \)

194. 28. 37. \(\infty \)

195. 28. \(\infty \)

195. 28. \(\infty \)

Para uno de los enlaces (ej el primero)

194.28.37. 000000: 00 → 1P de subred 000000 : 01 → 1P de interjaz de un router 000000 : 10 → 1P de interjaz del otro router 000000 : 11 → 1P de broadcant

```
· Para las LAN
```

25 direcciones IP { 25 = 32 : 5 bits host 3 bits de subred

máscara: 255.255.255.224

Dirección de cada subred

194.28.37. X

. 000 00000 × no sirve, ya la hemos wado 001:00000 → 32 010:00000 → 64

- 192

0 11:00000 -> 96

Dirección de broadcant de cada subred

194. 28. 37. Y . 001 : 1 1 1 1 1 → 63 . 010 : 111 11 → 95 0 11 : 111 11 → 127

Comandas curiosos:

ipconfig /all

netstat -r ⇒ vertablar de encaminamiento IP

arp -a ⇒ ver tabla ARP (dir IP ← dir MAC) se actualiza al hacer ping

tracert www.google.com ⇒ hace pings con distintos tiempos de vida 1,2,3,... y va escuchando a los distintos nodos que le avisar de la caducidad

2.4 Forwarding

Pos tipos de encaminamiento

DIRECTO: Si el destino esta en red a la que esta conectado INDIRECTO: Destino en red distinta (al menos un router intermedio)

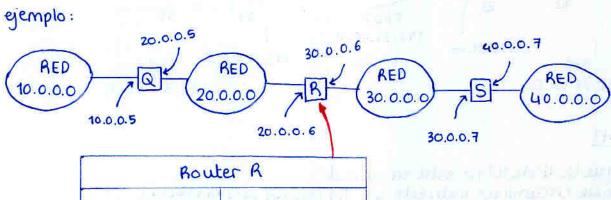
Directo:

. Necesario conocer la dirección física

· Para el paquete al nivel injerior (el cual lo encaprulara y se encargará de entregarlo)

Indirecto:

- · Necesario conocer la dirección física del router
- · Pasa el paquete al nivel injerior



Row	Router R			
Para alcanzar	Encaminar por			
20.0.0.0	Directo '			
30.0.0.0	Directo			
10.0.0.0	20.0.0.5			
40.0.0.0	30.0.0.7			

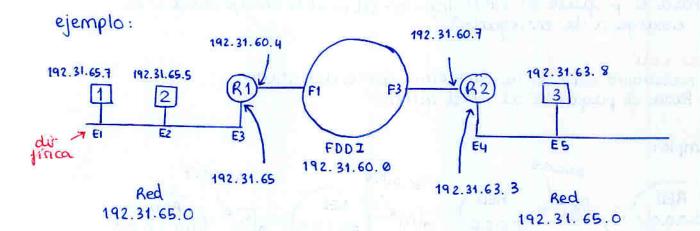
Algoritmo de encaminamiento

- 1. Extraer dir. IP destino (D) → obtiene prefijo de red (N) 1-a) si N directamente conectada - encaminamiento directo (obtiene du fisica destino y pasa al nivel injerior)
 - 1-b) si no er arí → encaminamiento indirecto
- · Ruta especificada para D enviar al salto indicado en tabla
- else . Ruta especificada para N "
 else . Ruta "por dejecto" enviar a dirección por dejecto
 else v. Error, se pierde el paquete

2.5. Protocolos auxiliares

= Address Resolution Protocol RFC 826

El ARP proporciona la dirección física a partir de la dirección IP a nivel enlace datos en la carga ARP Para ello hace un broadcast con la 1P destinova toda su red y aquel host que tenga dicha IP mandará la dirección física suya.



$H1 \rightarrow H3$

· H1 ve que la IP de H3 no esta en su red

· Tiene que encaminar indirecto por R1 (wsabe por sur tablar)

· Obtiene dirección fisica (E3) de R1 por ARP (broadcast dondola IP de R1 a roda su red, R1 responde con E3)

· manda al nivel injerior el cual encamina a la dir física E3 (en la carga del nivel inferior viajo el paquete IP con la dirección destino, no con la del router)

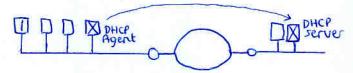
· a R1 llega trama que desencapsula y obtiene paquete IP · R1 ve que la IP de H3 no esta en su red

. Tiene que en caminar indirecto por R2 etc

RARP: reverse ARP. Obtiene IP a partir de dirección física (pero solo en propia red - requiere un servidor RARP por cada red) metoral I

BOOTP: Permite que la difusión traspase a otras redes (sólo necesario 1 BOOTP en el 115 lema) mejora Inconveniente: actualizar IPa mano

DHCP: Dynamic Host Configuration Probocol se pueden actualisar IP tarto manual como automático · se necesita DHCP agent (intermediario entre el que pide dirección 17 y el servidor DHCP) en cada red, pero sólo 1 servidor DHCP. · Permite asignación dinámica de direcciones IP



· ICMP

ICMP va en la carga de 17

Trama
Enlace Dates

MAC origen
MAC dentine
Paquete IP

ICM P

· Internet Control Message Protocol

· Refleja las buenas inténciones del servicio de Internet

Router monitorizan -> mensaje informativo al origen Mensajes de ICMP van sobre datagramas ip (alcance global)

Ejemplos de mensajes ICMP (www.iana.org/assignements/icmp-parameters)

· destino no alcanzable

. tiempo de vida agotado

· problemas en parametros

· control de congestión > choke packets

· eco/respuesta al eco (ping)

· Protocolos de control de encaminamiento

Encaminamiento adaptativo → gestionar y mantener tablas.

Internet se agrupa en sistemas autónomos comunicados por una red de pasarelas

(i.e. hay protocolos para dentro y para entre sistemas autónomos)

Ventajas { Tablas | mas pequeñas Ventajas { Tablas | facilità gestión y encaminamiento Recursos Red - Independiza diseño y administración

Dos tipos de protocolo IGP: Interior Gateway Protocol para encaminar dentro del sistema autónomo

EGP: Exterior Gateway Protocol para encaminar entre sisteman autónomos

- IGP :

· RIP: Routing Information Protocol AFC 1058

· Vector distancias (mide la distancia en saltos) Practicamente ya no se usa.

· OSPF: Open Shortest Path First RFC 2328

· Estado del enlace (recuerda: tiene info de toda la red)

· GGP: Gateway to gateway Protocol RFC 823

Vector distancia (distancia en saltos)

· HELLO : RFC 891

vector distancia (distancia en retardo)

- EGP:

· BGP: Border Gateway Protocol RFC 1771 y 1774 Vector distancia

3.1 IPV6 VS IPVU

· IPV4

· Ueva desde finales de los 70

· ha sobrevivido a avancer tecnológicos:

- procesadores más rápidos

- memorias más grasdes

- incremento disponibilidad ancho de barda

número de usuarios ha ciecido: se ha exprimido la capacidad de direccionamiento (subredes, NAT...)

· nec'esidad de evolucionar:

- tecnología siguesu avance

- nuevas aplicaciones con requerimentos de red mayores (ej: Hempo real)

- sigue oreciendo nº usuarios

En 1990 la IETF trabaja en nueva versión de IP Objetivos

- no quedarse sin direcciones

- redulcir tablar encaminamiento

-simplificar protocolo

- seguridad

- tipos de tráfico

- mejorar multicasting (en IPVL hay IGMP = gestion grupos)

· roaming sin cambiar dirección

· permitir evolución regura

- permitir coexistencia con 1PV4

Hicieron RFC 1150 - Solicitud propuestas Recibieron 22 propuestas cogieron 7 propuestas y las mezdaron

Características mais importantes de IPV6 (RFC 2460...2466)

· direcciones más largas (128 bits)

· simplifica la cabecera (7 campos) (habiar 13 en 1844)

· mejora soporte opciones

· mejora seguridad < privacidad: permite encriptado

· se pone man incapié en la calidad del rervicio

3.2 Direccionamiento

16 bytes (128 bits) (7 10 16 1P's portada mmo de la tierra)

8 grupos de 4 digitos hexadecimales y separados por ::

8000 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF

: = simply cación

se compatibiliza con 1Pv4 haciendo :: 192.31.20.46

3.3. Formato Datagrama

La idea er poner en la cabecera bare la extrictamente necesario y tener la opción de añadir cabecerar de extensión

Cabecera Base (40 bytes)	Cabecera de extensión 1	cop. de	Some Authorized
, spin a	Opcion	al	- 1-14th may recorded

7 15 23 31

Flow Label { 20 bits Aseudoconexioner)

Payload Length { 16 bits - 64k Tamaña en bytes sin Contar cabecera base

Next { 1 byte Header { Indica tipo signiente cabecera Si es la ultima indica el protocolo

Hop Sibyte Limit Tiempo de vidade paquete en saltos

· La fragmentación se implementa como cabecera de expansión · No hay checksum

Cabecerar de extensión · Información extra opcional van despues de cabecera base · No deben ir en un orden, pero se sugiere: - Hop-by-hop options: se lee esta cabecera encada salto - Destination options - Routing - Fragmentation - Authentication Encripted security Payload Todas ellas comienzas igual: - next header - header length extension Header Length Next Header (Length) (Type) Extension Langitud sin contar los 8 primeros octetos byte Type byte Length rento Value Para las cabeceras que tiener opciones les sigue: · Hop-by-hop otions: todas routers deben saberlo - Tumbo Payload opción datagraman > 64k (se pueden poner muchan) Next Header 194 Jumbo Payload Length (en la cabecera base) · Destination options: aun no se han pensado, pero se levan sólo en destino. - Routing

Routing Type: 0

Reserved

Lista de direcciones IP

segments Left

· Fragmentation

no transparente (la ensabla el destino)

· solo puede tragmentar el origen (ei: nodo avisa a origen: paquete demasiado grande; el origen tragmenta y vuelve a enviar)

Next Header	(Reserved)	Fragment Offset	L
lder	itification		

- Authenthication

uso de técnicas criptográficas para estar seguro de la identidad del emisor.

- Encripted security payload

uso de técnicas criptográficas para encriptar el contenido de un paquete.

Junio 2003

Fragmentación (compo Fragment Offret)

Problema 5

Paquete IPV4 de 3000 bytes debe fragmentaise en MTU = 500 bytes

2980 de datos 20 de cabecera

4:80 de datos 20 de cabecera

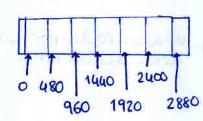
a) écuántos fragmentos?

6 fragmentos de 20 + 480 bytes 1 fragmento de 20 + 100 bytes

b) ¿ Qué información de fragmentación lleva la cabecera?

Identification: identificación para distinguir al paquete original todos los fragmentos el mismo valor

Fragment Offset:



cada fragmento pondrá el número de su primer octeto

DF: dont fragment: activado en todos

MF: more fragments: Todos activados menos el último

- c) Fragmentación transparente us. Fragmentación no transparente
 - El destino puede olvidare del ensamblado
 - · Todos los fragmentos deben ir por mirma red para que el router de ratida los ensomble
- · Los fragmentos pueden ir par dende quieran
- · El destino debe ensamblarlos

Desventaja comun: si se pierde un tragmento se deshecha todo el paquete

Junio 2004

Cuestion

. N nodos mallados con conectividad total

· Encaminamiento plano (no jerarquico)

¿ De que tamaño en la tabla de cada uno de ellos?

N-1 ⇒ una entrada por cada uno de los destinos

· si dividimos en dos areas de $\frac{N}{2}$ y hacemos encaminamiento jerárquico

¿ De que tamaño en la tabla de cada uno de ellos?

 $\frac{N}{2}-1 \Rightarrow \frac{1}{2}$ una entrada por cada destino de su área

+

1 ⇒ Una entrada por cada
área de dentino

Total: 1/2

¿ aus vertajos de eficiencia tiene cada orterio?

- . El segundo en man ejectivo en cuanto a tamaño de las tablas
- · El primero es mais ejectivo en cuanto a encamina niento

Septiembre 2004

Problema 2.

Ping -> ICMP { echo request echo reply

158, 62, 33, 23 Dir IP:

158.62.44.25

Máscara: 255.255.240.0

255. 255. 240. 0

MAC: 00:08:0D:80:32:11

00:08:EB:11:BB:CD

Pararela: 158.62.32.1

158.62.32.1

Escribir la secuencia de paquetes

1. Encommaniento directo? == misma subred?

Operación del AND con la máscara para obtener la subred

158.62.33.23 00100001

misma subred.

11110000

1111 0000

158.62.32.0

Tambien podia sabesse viendo que tienen la misma pasarela por dejecto (que sien pre

255. 255. 240. 0

158.62.44.25

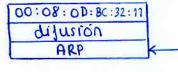
158.62.32.1 0010 1100

enta en tu sub red)

Vemos que están en la misma subred. · A hard encaminamiento directo a B

· A hará ARP preguntando que dirección física tiene la IP de B.

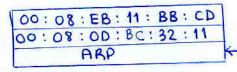
origen destino info



158.62.33.23

158. 62. 44. 25

· B contestará con trama AAP



158.62.44.25

158.62.33.23

Ahora A ya puede envior a B el paquete IP con ICMP (encapsulado en nivel 2 conociendo mác origen y destino) 00:08:0D:BC:32:11

00: 08 : EB : 11 : BB : CD 158.62.33.23 158. 62.44.25 IP ICMP (echo request)

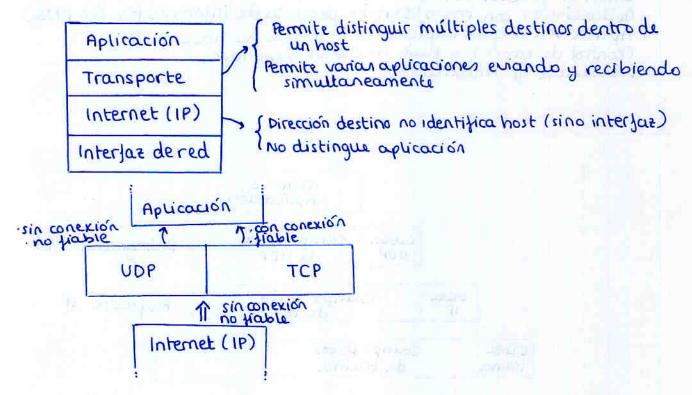
Y B responde a A

00: 08 : EB : 11 : BB : CD 00:08:0D:BC:32:11 CALL CONTRACTOR OF THE PARTY OF 158.62.44.25 IP 158.62.33.23 ICMP (echo reply)

DEAD TO MORE OF THE

Tema 7 UDP/TCP

1. Introducción



Puertos:

50 - multitarea - varios procesos simultaneamente

Puerto de protocolo

· punto abstracto de destino

· numero entero positivo

so proporciona interfaz proceso-puerto

· acceso sincrono: ejecución de programa se detiene cuando se escucha un ·memoria (cola espera) por si ningun proceso reclama algo que ha llégado a un puerto

destino = dirección IP + puerto

2. UDP

2.1 Generalidades

·UDP - User Datagram Protocol **RFC 768**

· Proporciona servicio no orientado a conexión y no fiable · no garantiza que segmentos UDP llegues · pueden haber duplicados

· no garantiza entrega en orden

· no hace control de congestion

2.2. Usos

Aplicaciones tiempo real y multimedia

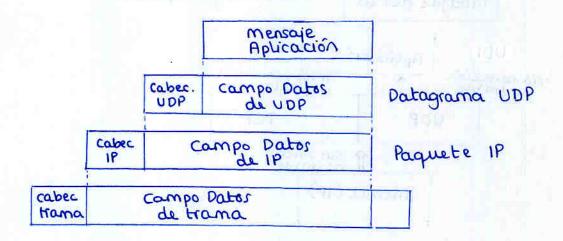
· Entornos fiables (LAN)

· Aplicaciones con transferencia pequeña de información (ej DNS)

(control de errores y Jujo en capas superiores)

Broadcast y multicast

2.3 Encapsulado



2.4. Formato

Cabecera	Datos	the first attendate about
1 8 bytes		wanted and name of
A Property of	Linguista Street	
		15 man Line and the Contract of the Contract o
Source Port	arely zers	

source Port { 16 bits opcional

Destination Port: puerto UDP dentino

Checksum { 16 bits opcional

Length: 16 bits no de byter cabecara + datos min: 8 byter

min: 8 bytes max: 64k bytes

nota: en 1Pv4 sólo cabecara

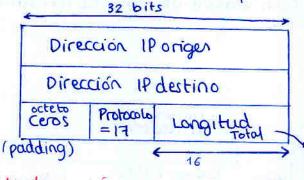
· en IPv6 no hay

· en UPP hay checkrum de cab + datos + pseudocabecera

en TCP igual

· En VDP en opcional (todo ceros > no se una = red fiable)

Para generar y comprobar el checksum se genera una pseudocabecera (que en realidad no se envia) que es:



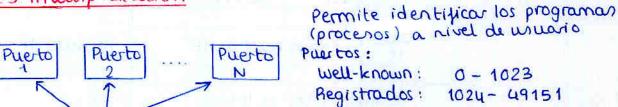
vulnera un poco la división en capan pero nos aregura que se ha Uegado donde había que Uegar.

longitud del datagrama en bytes

2.5 multiplexación

UDP

Capa 1P



Asignación : u

49152-65 535

www. iana.org/assignments/port-numbers

ej 80 para http 110 para POP 21 para FTP

3, TCP

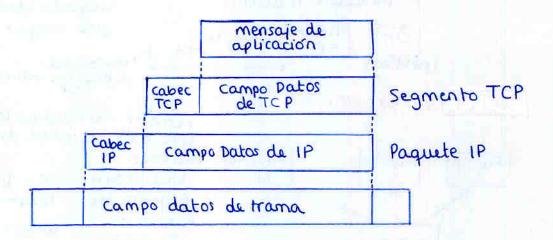
3. 1 Generalidades

- AFCs 2581, 2018, 1323, 1122, 793
- · orientado a conexión :
 - · establecimiento, transferencia y liberación
 - · full duplex
- · Fiable
 - · garantita entrega en orden
 - · no hay duplicados
 - · no hay perdidas (retransmisiones)
- · usa puertos igual que UDP
- · TCP utiliza el concepto de conexión como abstracción
 - · se define como ambos extremos de la conexión

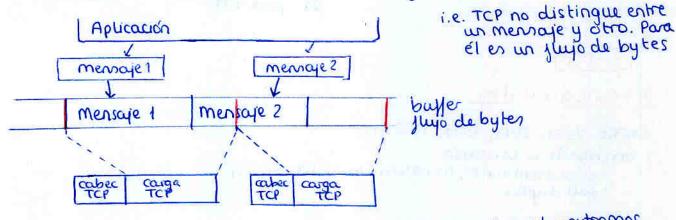
(1P + puerto)

· permite multiplexación por conexión (i.e. puede tener varias conexiónes en un único puerto, o TCP las puede distinguir perfectamente) · consigue servicio con conexión y fiable utilizando:
- reconocimiento positivo con retransmisión
- ventana deslizante (con tamaño de ventana dinâmico)
4 optimiza los recursos

3.2 Encapsulado



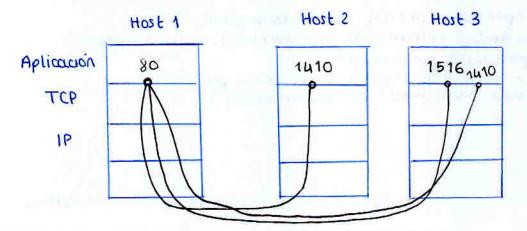
Flujo no estructurado El sólo transmite un flujo de bytes (memoria intermedia entre aplicación y TCP): un mensaje de TCP puede tener por tanto mensajes distintos en un mismo segmento



3.3 multiplexación

Conexión = Se define por 2 puntos extremos = punto origen + punto dentino

cada conexión se controla independientemente Por tanto pueden entablecare multiples conexiónes sobre un mismo puerto (a diferencia de UDP)



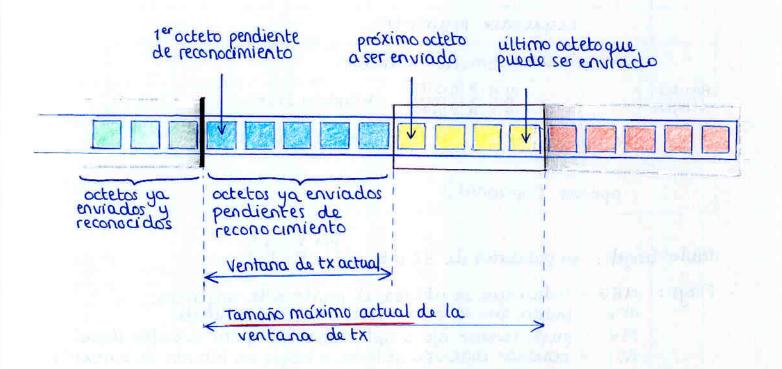
i.e. TCP asocia los mensajes entrantes con una conexión, no con un puerto.

La conexión se define con sur dos puntos extremos

punto = IP + nopuerto extremo = dirección de transporte

3.4. Secuenciamiento

· TCP trata el flujo de datos como una secuencia de octetos (bytes) · Implementa ventana deslizante contando octetos: Guarda 3 punteros:



3.5. Formato

Seg mento TCP

Cabacera Patos

· Parte fija: 20 bytes

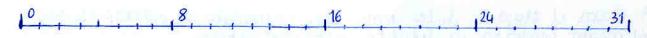
· Parte de opciones : - puede no induir ninguna

- relleno (padding) hasta multiple 32 bits

opciones mais importantes:

· MSS: maximum segment Size

NAK: negative ACK; permite implementar repetición selectiva (RFC 1106)



Source Port		Destination Port	
	sequence Number	er mandan = mass	
Ackn	www.ledgement No	umber	
Header Length RCSSYN Window Size			
Checksu	m	Urgent Pointer	

options (optional)

Header Length: en palabras de 32 bits (i.e. 5-15)

Flags: URG - Indica que se utiliza el puntero de urgencia

ACK - Indica que se está hacierdo reconocimiento

PSH - push (envior info a aplicación sin esperar a buffer lleno)

AST - resetear conexión abierta o negar un intento de conexión

SYN - para establecimiento de conexión

FIN - para cerror conexión

Window Size: el receptor indica al transmisor el tamaño maximo que debe tener su ventana (permisos) en ere instante (i.e. el tx no va moviendo su ventana según va enviando para mantener el tamaño maximo, sino que el final se queda quieto hanta que uega un nuevo windowsize) Por tanto er el nº de bytes que el receptor quier recibir contando derde el ACK number.

Checksum: se aplica a cabecara + datos + preudocabecera

can campo chederum a ceros Source 1P address
Destination 1P address
O's Probool TCP segm. centh

Puntero de urgencia: permite enviar datos jura de banda (sin tener que guardar el orden)
s. URG=1, ente puntero indica el final de los datos urgentes.

3.6 Control de Flujo

- · Ventana derlizante de tamaño variable (sistema de créditos: tamaño (window size) viene dado en los ACK.
- · Es independiente para cada conexión y para cada sentido de una misma conexión.

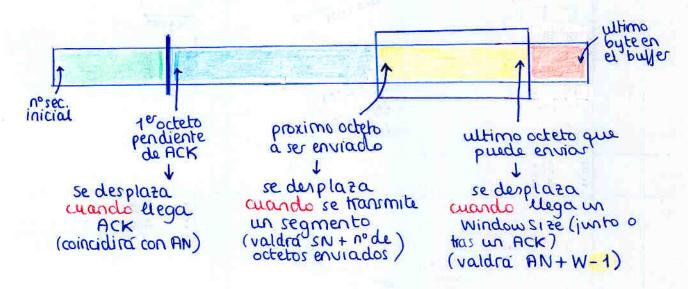
SN: sequence number: n° del primer octeto del segmento TCP

AN: ack. number: no de octeto que esta esperando

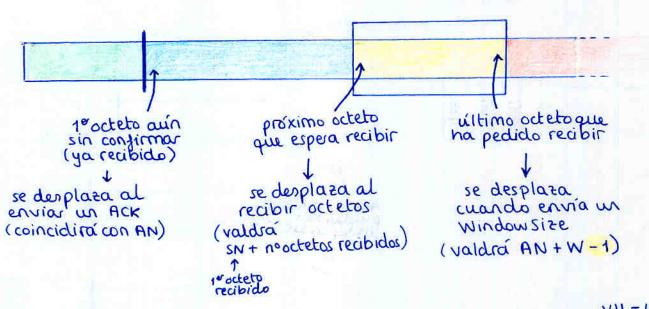
→ se confirman hanta et i-1 (inclusive) W: window size : no de octetos que el receptor pide dende et i (AN)

ei:
$$AN = i$$
 \Rightarrow receptor quiere octetor $[i, i+j-1]$
 $n \circ de octetos = (ultimo - primero) + 1 = j$

En transmisión:

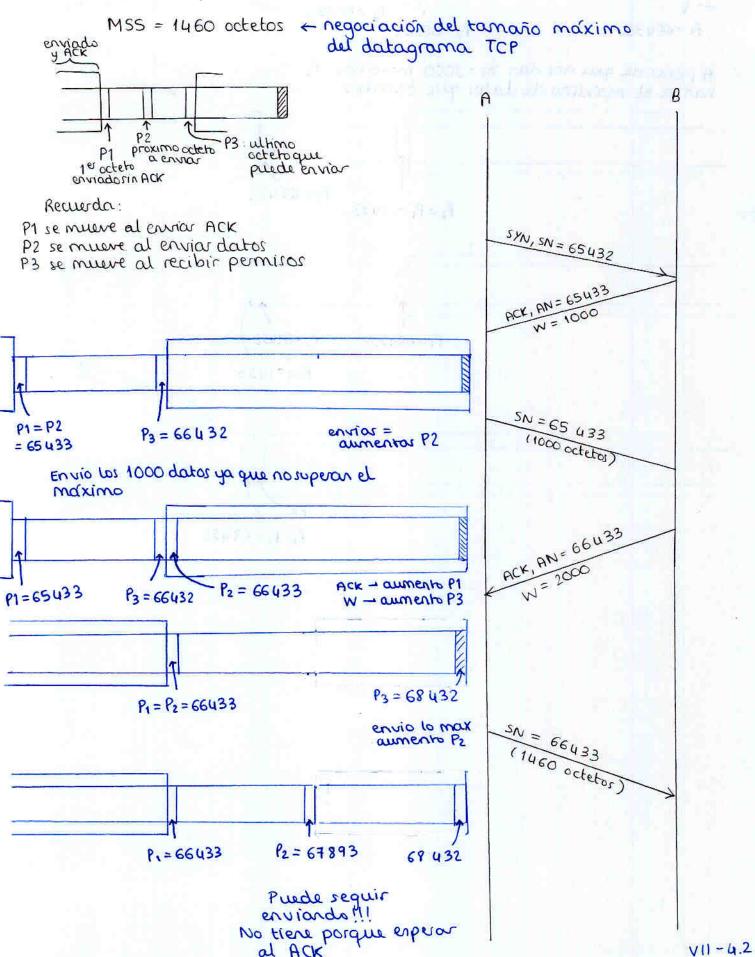


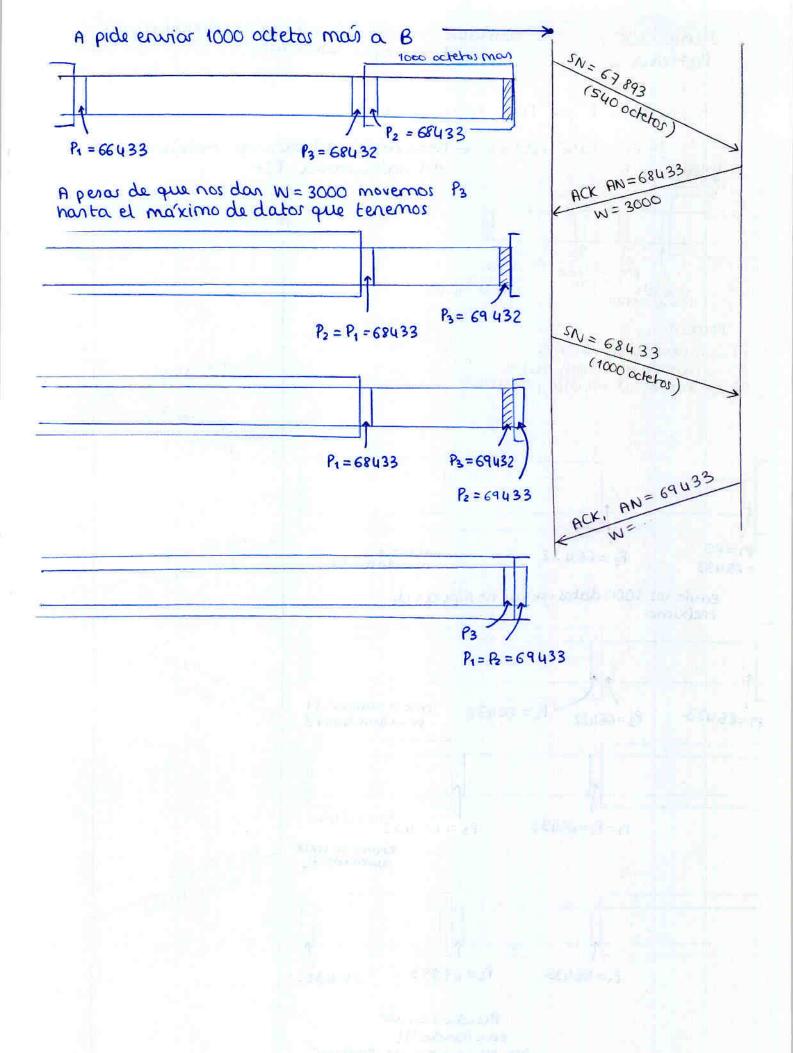
En recepción



Junio 2005 Problema 1 cuidado: no usa la misma nomendatura que el ejemplo anterior

A envía a B por TCP 3000 octetos



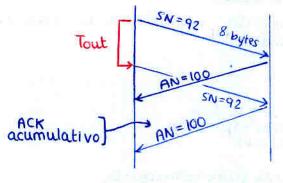


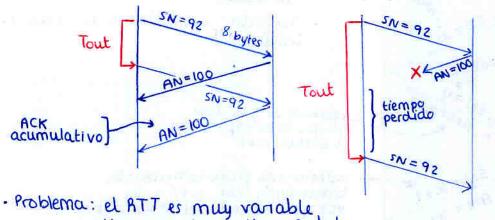
3.7 Temporización

Calculo del timeout

No debe ser ni muy pequeño, ni muy grande.

caro ideal: poco mayor que (Round Trip Time)





RTTmuestreads:

· monitoriza tiem po entre transmission y ACK.



M RTT muer treado ATT estimado

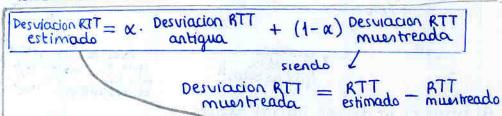
No se calcula cuando hay retransmisión o ACK acumulativo para no conjundirse.

= a. RTT + (1-x). BTT
mustreado estimado antique para suavizarlo.

- A partir del ATTertimado obtenemos el Time Out:
- Antiquamente:

Time Out = B. BTT

se recomendaba B=2



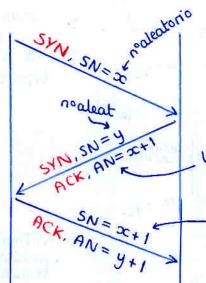
- Actualmente:

Time Out = RTT estimado + 4. Desviación RTT estimado estimado

lógico: si RTT cambia mucho; Tout debe ser >> que RTT; pero si RTT en cte, Tout = RTT

3.8 Establecimiento de la conexión

Utiliza un protocolo a 3 bandas



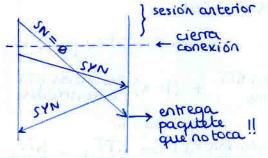
- · Garantiza que ambos extremos están listos para la entrega de datos.
- . Acuerdar un número de secuercia inicial.

le reconoce x y le dice que ya está esperando el octeto x+1

aprovecha para comenzar la transmirión con x+1 a la vez que reconoce el nº rec del obro.

soluciona los problemas de la conexión a 2 bandar, en el cual segmentos de la sesión anterior ya cerrada podrán interjerir

ej: a 2 bandar sin número de secuencia: segmento de datos obsoleto ej: a 2 bandar con número de secuencia: segmento SYN obsoleto



Al hace et no de sec inicial aleatorio las possibilidades de que esto ocurra son casi rulas (recueda IN es de 32 bits)

ente ve

que el

Act z+1

cree que ambos

están de acuerdo

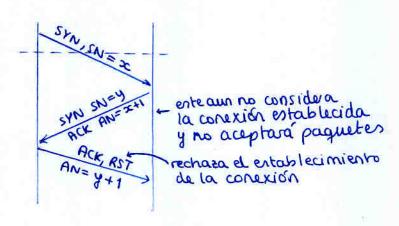
en nº de sec

el RST uega

demanidado

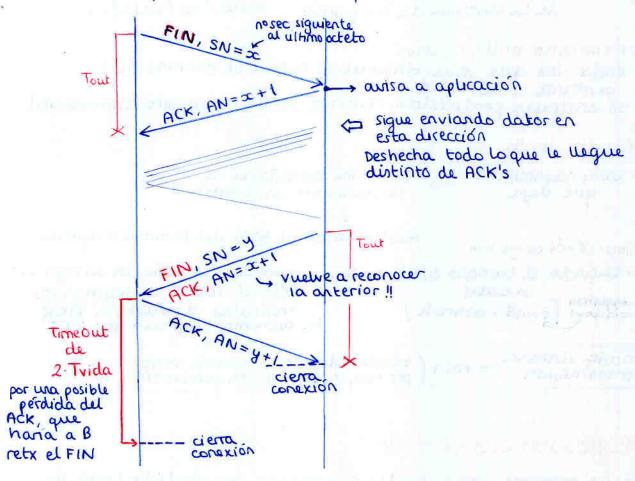
tarde

Con 3 bandar ne soluciona



3.9 Liberación de la conexión

se ciera el prijo independientemente para cada sentido



3.10. Control de la congestion

Problema: En principio TCP (siendo extremo a extremo) no sabe si hay congestión en la red. TCP solo observa el vencimiento del Tout, y las retransmisiones consecutivas sólo agravas el problema.

solución: TCP infiere que los vencimientos de Time out se deben a la congestión y actua para reducir el tráfico.

TCP actua en 2 frentes:

TCP asume que la mayoria de segmentos perdidos se debe a la congestión

1 calculo del Timeout

Algoritmo de Karn; combina:

- Ignorar retransmisión al estimar RTT

(ya que el ACK que se recibe podría ser de la 1º transmisión o de la retransmisión)

No se mide el RTT para segmentos retransmitidos

- Timer-backoff:

se incrementa el timeout cada vez que se retransmite un segmento Timeout = B. Timeout

hasta que llega el ACK de un segmento que no ha sido retransmitido.

V11-6

2- Control de flujo: ventana de congestión

Timeout - Decrecimiento multiplicativo _ arranque lento para de la ventara de congentión evitar oscilaciones

Decreamiento multiplicativo:

cada vez que vera timeout se reduce el tamaño de la ventara a la mitad. Si continuar perdiéndose ocurrirá un decrecimiento exponencial

Arranque lento:

4 cada reconocimiento - aumenta tamaño de la que llega ventana en un regmento

Prevención de congertion

Hanta llegar al 50% del tamaño o riginal

Li Cuando el tamaño en del 50%

en malidad

solo si ToDos los segmen tos

en malidad

solo si ToDos los segmen tos

enviados devuelven ACK

i.e. aumenta 1 segmento por RTT

Tamaño ventara = min (tamaño indicado tamaño ventara)
de transmisión = min (por receptor (W), de congentión)

3.10 Recuperación de caidas

cuando un extremo cae y vuelve a arrancar, ha perdido toda la información de entado.

El cado no afectado todavía cree que sigue conectado

Dos opciones:

· Temportzador de renuncia: si el lado activo está demasiado tiempo sin recibir ACK, ciera la conexión e informa al usuario.

· El caido responde con bit RST a cada regmento que recibe. Al recibir RST el lado activo, cierra la conexión

El usuario debe decidir cuando y como reabrir la conexión (pueden haberse perdido datos o recibido duplicados)

TELEMATICA. 7 de Septiembre de 2005. al verilem un liseau la magnicia sema al sels tempos de la

Dpto. de Comunicaciones. E.T.S.I. de Telecomunicación de Valencia.

- Duración del examen: 2 horas.
- Para las cuestiones de test:
 - Responda en la hoja especial para su lectura óptica usando lápiz.
 - Las preguntas contestadas correctamente valen 0,2 puntos, las contestadas incorrectamente restan 0,067 y las no contestadas no puntúan.

· Sólo hay una opción correcta por pregunta.

- Para las restantes cuestiones utilice sólo el espacio destinado a respuestas.

- Las respuestas deben realizarse con bolígrafo o pluma.

- Se invalidarán las respuestas que no cumplan los requisitos indicados.

Δ	P	FТ	.1	ID	OS.

NOMBRE:

TEST (4 puntos)

1.- En el buffer de emisión de TCP de un host A se utilizan tres punteros: P1 indica el primer octeto enviado pendiente de reconocimiento, P2 es el último octeto enviado y P3 el último octeto que se puede enviar. Si en un momento dado P1=2156, P2=2460 y P3=3000 y el host A envía un segemento, ¿Cual será el número de secuencia de ese segmento?

- a) Número de secuencia = 2460
- b) Número de secuencia = 2156
- Número de secuencia = 2461
- d) Depende del tamaño máximo del segemento

2.- En el ejemplo anterior, ¿cuál es el útimo valor que envió el host remoto al host A en el campo Window?

P3 = P1 + W - 1

- a) 541
- b) 540
- c) 844
- (d) 845

3.- La dirección IPv4: 158.42.3.255, es de difusión si:

- a) Es una dirección clase A con algún tipo de subnetting
- b) Es una dirección clase B con algún tipo de subnetting
- c) Es una dirección clase C con algún tipo de subnetting
- d) Es una dirección clase Multicast

clase A: 0

R: 10

r: 110

0 . 4 4 1 0

D: 11

4.- Indique la afirmación correcta con respecto a la técnica de encaminamiento por inundación:

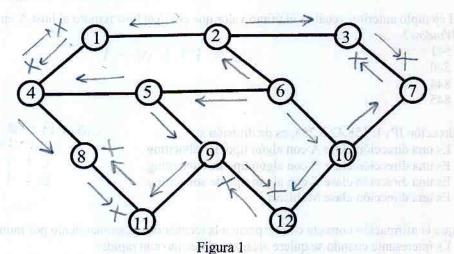
a) Es interesante cuando se quiere alcanzar el destino con rapidez

- b) La sobrecarga de paquetes en la red es mínima, ya que no requiere intercambios de información de control entre nodos
- c) Es incompatible con otras técnicas de encaminamiento
- d) Es una técnica exclusivamente de difusión

5.- Respecto al algoritmo de encaminamiento distribuido del estado del enlace:

- a) Es suficiente con que cada nodo conozca el coste de los enlaces a sus nodos advacentes
- b) Todos los nodos tienen que conocer todos los costes de todos los enlaces de la red
- Se ejecuta en un nodo central que calcula las tablas de todos los nodos y posteriormente envía a cada nodo su tabla correspondiente
 - d) Las tablas que genera no son óptimas

- 6.- Control de la congestión en el nivel de red de la arquitectura TCP/IP:
 - a) No se implementa por ser una red altamente fiable
 - b) Utiliza una técnica tipo Leaky Bucket
 - c) Utiliza una técnica tipo Token Bucket
 - d Ninguna de las anteriores es cierta
- 7.- La cabecera de UDP consta de:
 - (a) 2 palabras de 32 bits
 - b) 3 palabras de 32 bits
 - c) 4 palabras de 32 bits
 - d) 5 palabras de 32 bits and la servicio de la companya del companya de la companya de la companya del companya de la companya
- &- Respecto al intervalo de medida de Frame Relay indique qué afirmación es cierta:
 - a) No afecta al número de tramas que se envían con el bit DE=0
 - b) Cuánto mayor sea el intervalo de medida mayor será el CIR asignado
 - c) Varía para cada trama transmitida
 - d) El tamaño de ráfaga permitido depende del valor de este parámetro
- 9.- Control de la congestión por Paquetes de Restricción (Choke Packets):
 - a) Tras la recepción del primer paquete de restricción, vencido el primer temporizador y hasta que venza el segundo, la recepción en el Host de nuevos paquetes de restricción será ignorada a efectos de reducir la tasa de tráfico generada
 - b) Es una técnica híbrida entre Leaky Bucket y el descarte de paquetes
 - Si en un router en la última monitorización de un enlace se superó el valor de utilización umbral, no se realizarán más monitorizaciones hasta que no venza el primer temporizador
 - d) Ninguna de las anteriores es correcta



10.- Sea la malla de la figura 1. Considerando operativas unas tablas de encaminamiento por camino más corto óptimas, si hacemos una difusión (con la técnica de Spanning Tree Adaptativo ó Dinámico) desde el nodo 6, el número de copias generadas (veces que el paquete a difundir es transmitido por un enlace) es:

- a) 12
- b) 15
- (6) 19
- d) No se puede determinar, depende de cual sea el árbol

11 0	Con respecto a las técnicas de control de encaminamiento aisladas:	
a) No existen tales técnicas	
	Generan una sobrecarga de tráfico de control excesiva, como sucede con la Inundación	
c	Sólo se pueden implementar en redes IP cuando se va a utilizar el protocolo UDP	
đ	Ninguna de las anteriores es correcta	
	manufacture as a mark who led solutions is field as some TM as some I as	
a h	Es un protocolo con conexión no fiable l'improduction de la	
U) Sólo proporciona un servicio de transferencia fiable, mientras que si se quiere un	
	servicio con conexión hay que recurrir a otros protocolos con conexión a 3 bandas	
C	Los bits SYN y FIN nunca pueden estar activos en el mismo segemento	C
	Los bits SYN y ACK nunca pueden estar activos en el mismo segemento	
	estandes ascregio al de fransació de a contracto de contracto que sumas distrogramaçe mem le	
	ndique que arquitectura es correcta:	
	Web (HTTP)/UDP/ICMP/IP/LAN (Ethernet)	
) Web (HTTP)/Frame Relay/IP/LAN(Ethernet)	
	Web (HTTP)/TCP/IP/LAN (Ethernet)/Frame Relay	C
ď	Web (HTTP)/UDP/TCP/IP/LAN(Ethernet)	
14 D		
	Respecto al protocolo ARP:	
a	Es un protocolo auxiliar de IP que se utiliza únicamente en los routers	
b,	En las tablas ARP sólo aparecen entradas estáticas que se deben incluir de forma	
man, ni	I = Jin la figura signicute se represent la solution de la ren de constitica ión launam e	
c)	Las tablas ARP asocian direcciones IP origen y destino de dos interfaces que	
9	pertenezcan a la misma red de área local	
U d)	Los paquetes ARP request y ARP reply tienen el mismo formato	d
	TOWN AND ADDRESS AND ADDRESS OF A DESCRIPTION AND ADDRESS OF ADDRESS OF A DESCRIPTION AND ADDRESS OF A DESCRIPTION ADDRESS OF A DESCRIPTION AND ADDRESS OF A DESC	
15 L	Ina de las diferencias entre el formato de los paquetes de IPv4 y de IPv6 es que:	
a)	IPv6 utiliza dos palabras de 32 bits para cada una de las direcciones IP origen y destino	
	mientras que IPv4 sólo utiliza una para cada dirección	
b)	IPv4 permite añadir opciones a la cabecera mientras que IPv6 no	C
c)	En IPv6 desaparece el campo del checksum que aparecía en la cabecera de IPv4	
d)		
4.7 5		
	Il campo window de la cabecera de los segmentos TCP se utiliza:	
	Para el control de flujo	
	Para el control de la congestión	4
(c)	Para el control de flujo y para el control de la congestión	a
d)	Ninguna de las respuestas anteriores es correcta	
1	Condertion to natur	
N E	n el algoritmo de encaminamiento de estado del enlace:	
(a)	El bucle se repite tantas veces como nodos destino haya en la red	
	El bucle se repite hasta alcanzar el diámetro de la red	
c)		
d)		
(4)	vecinos.	
	To the same of the	
18 - C	onsiderando la malla de la figura 1, el diámetro de la misma es:	
a)		
b)	the to-public or the sounders police 12, pool or contra	
c)	d No deberia rer 12-1!	
d)		
u)	110 be passe determinat, depende de la tecinea de encaminamiento	

19.- Cuál de las siguientes afirmaciones respecto a los protocolos de transporte TCP y UDP es FALSA:

a) En TCP se pueden establecer varias conexiones utilizando la misma dirección IP destino y el mismo puerto destino

b) En UDP, al igual que en TCP, se transmiten flujos de datos no estructurados

c) Tanto en TCP como en UDP el cálculo del checksum se realiza utilizando una pseudocabecera

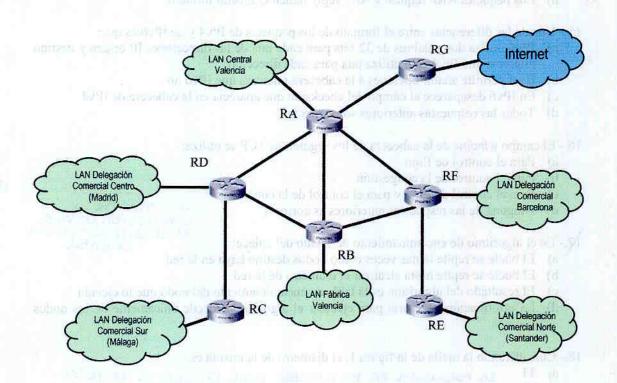
d) La cabecera de TCP tiene una longitud mayor que la de UDP

20.- Una red de conmutación de paquetes está formada por 3 routers colocados en serie y dos hosts conectados a cada uno de los routers de los extremos. Todos los enlaces de la red son de R bps. Un host envía al host remoto un paquete de longitud L. Suponiendo despreciables todos los retardos excepto el de transmisión, ¿cuál será el retardo que sufrirá dicho paquete hasta llegar al otro extremo?

- a) 3L/R
- b) 4L/R
- c) L/3R
- d) L/4R

CUESTIONES Y PROBLEMAS (6 puntos)

1.- En la figura siguiente se representa la solución de la red de comunicación de datos de una empresa valenciana.



(puerto + IP) origen + (puerto + IP) destrino

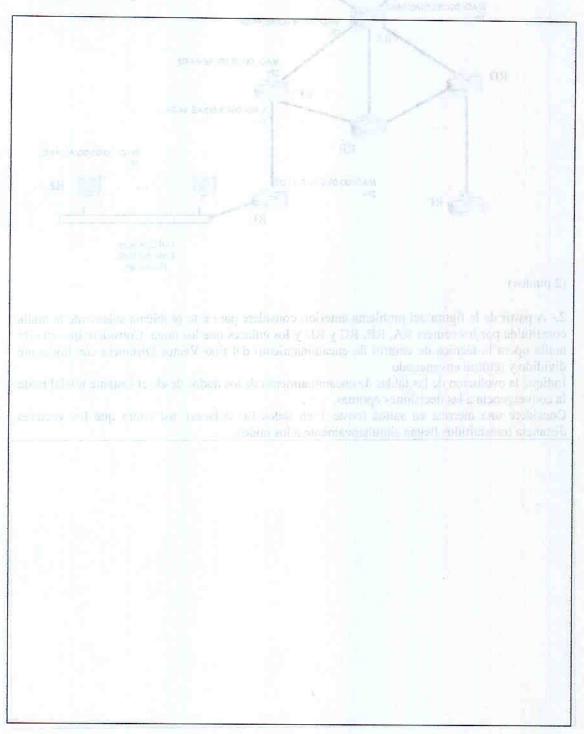
b

b

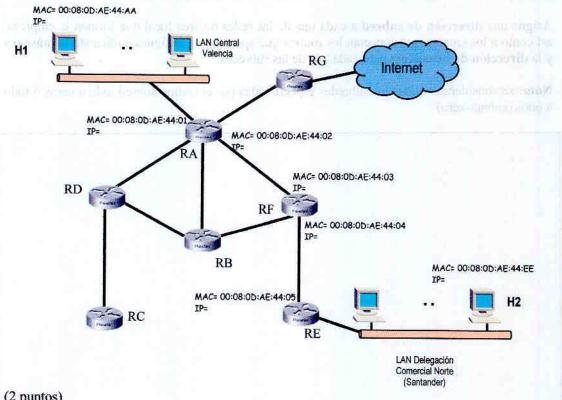
Dicha empresa tiene asignada la dirección de red de clase C 194.28.37.0. En cada una de las redes de área local de la empresa se necesitan asignar direcciones IP a 25 interfaces para lo cual es necesario dividir el rango de direcciones disponible en subredes.

Asigne una dirección de subred a cada una de las redes de área local que forman la empresa, así como a los enlaces que conectan los routers que aparecen en la figura, indicando la máscara y la dirección de broadcast para cada una de las subredes.

Nota: se consideran válidas las subredes especificadas por el campo subred todo a ceros o todo a unos (subnet-zero)



Una vez dividido el rango de direcciones, asigne una dirección IP a las interfaces de red señaladas en la siguiente figura:



(2 puntos)

2.- A partir de la figura del problema anterior, considere para este problema solamente la malla constituida por los routers RA, RB, RC y RD y los enlaces que los unen. Considere que en esta malla opera la técnica de control de encaminamiento del tipo Vector Distancia con horizonte dividido y retorno envenenado.

Indique la evolución de las tablas de encaminamiento de los nodos desde el instante inicial hasta la convergencia a las decisiones óptimas.

Considere una métrica en saltos (coste 1 en todos los enlaces), así como que los vectores distancia transmitidos llegan simultáneamente a los nodos.

a- Se deficine de lan token backet oon une enganten te tu Slate 1 as tokens se jandam inzim de 20 Milys y tit velocritad de malago del tok ar coeken en de 1900 de sa Con minaro de stasvigar el militor az excloca a la saltim del tiben ha ke, un fembrio incide acciona velocadad de salida es 40 Milys i la cantestastada buffier e de 10 Milys i a un monor uno dado il an usu rajones de 10 Milys de 10 Milys a la cantestastada buffier e de 10 Milys i a un monor uno dado il an usu rajones de 10 Milys d

All Explored modest countries of the riests credition 21 is military contries because the six and a second countries in the six and a second c

both from the U.S. Settlem of at the Product of sector P444

on bill the military in bank makes 14 (o

(2 puntos)

(2 minus)

- 3.- Se dispone de un token bucket con una capacidad de 10 Mbits. Los tokens se generan a razón de 20 Mb/s y la velocidad de ráfaga del token bucket es de 200Mb/s. Con objeto de suavizar el tráfico se coloca a la salida del token bucket un leaky bucket cuya velocidad de salida es 50 Mb/s y la capacidad del buffer es de 10 Mbits. En un momento dado llega una ráfaga de 10 Mbits a la entrada del token bucket. ¿Cuánto tiempo tarda en transmitirse la ráfaga en cada uno de los casos siguientes?
 - a) El token bucket está vacío (no tiene créditos disponibles cuando llega la ráfaga)
 - b) El token bucket está a la mitad de su capacidad
 - c) El token bucket está lleno

TELEMATICA. 7 de Junio de 2005.

Dpto. de Comunicaciones. E.T.S.I. de Telecomunicación de Valencia.

- Duración del examen: 2 horas.
- Para las cuestiones de test:
 - Responda en la hoja especial para su lectura óptica usando lápiz.
 - Las preguntas contestadas correctamente valen 0,2 puntos, las contestadas incorrectamente restan 0,067 y las no contestadas no puntúan.
 - Sólo hay una opción correcta por pregunta.
- Para las restantes cuestiones utilice sólo el espacio destinado a respuestas.
- Las respuestas deben realizarse con bolígrafo o pluma.
- Se invalidarán las respuestas que no cumplan los requisitos indicados.

APELLIDOS:

NOMBRE:

TEST (4 puntos)

- 1.- La fragmentación con IPv4
- es no transparente,
 - b) en general es transparente, pero es no transparente cuando hay tunnelling,
 - c) puede ser transparente o no transparente, depende de si el flag correspondiente está o no activado.
 - d) Ninguna de las respuestas anteriores es correcta.
 - 2.- Indique la afirmación FALSA con respecto a la técnica de encaminamiento por inundación:
 - a) es interesante cuando se quiere alcanzar el destino con rapidez,
 - b) la sobrecarga de paquetes en la red es mínima, ya que no requiere intercambios de información de control entre nodos,
 - c) se utiliza como base en otras técnicas de encaminamiento,
 - d) es una técnica aislada.
 - Encaminamiento ierárquico:
 - a) Las redes con estructura jerárquica son menos sensibles a los problemas de congestión que las redes sin esta estructura (jerarquía plana o un solo nivel jerárquico).
 - b) Las redes jerarquizadas mejoran la eficiencia del encaminamiento (forwarding) por las implicaciones que tienen en las tablas de encaminamiento.
 - c) Las redes jerarquizadas garantizan enrutados óptimos, ya que siempre se trabaja sobre las rutas más cortas entre dos nodos cualesquiera.
 - d) Todas las afirmaciones anteriores son ciertas.

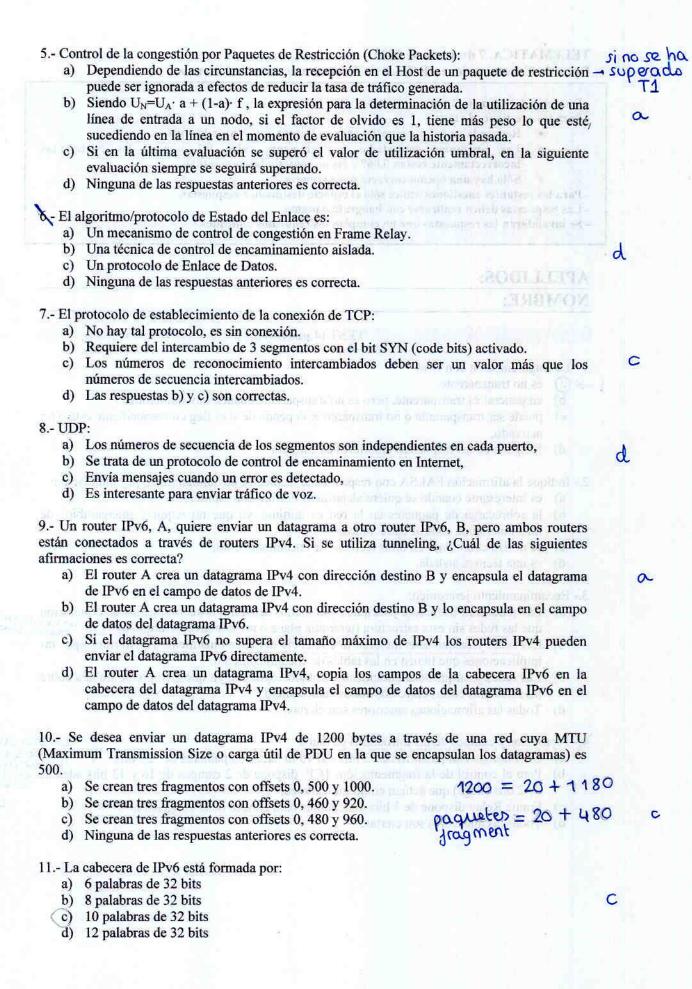
 - Protocolos y campos de las estructuras de datos: a) IPv4 trabaja con palabras de 32 bits e IPv6 lo hace con palabras de 128 bits.

 Pero co
 - b) Para el control de la fragmentación, TCP, dispone de 2 campos de 16 y 13 bits además de 2 bits (flags) que actúan como indicadores.

seri CE-state enviolent at 16

- Frame Relay dispone de 3 bits indicadores para control de la congestión.
- d) Todas las anteriores son ciertas.

C



12.- En Frame Relay: a) El nodo conmutador Frame Relay al que está conectado el equipo del usuario realiza una monitorización del tráfico que el usuario inyecta en la red por cada circuito virtual b) El equipo de usuario filtra el tráfico que va a enviar a la red Frame Relay para asegurarse de que no va a superar la velocidad de información comprometida CIR. c) El CIR es un parámetro que se va a adaptando a las situaciones de congestión de la red. d) Si se contrata un circuito virtual permanente no es necesario configurar el CIR. 13.- Si la llegada de un paquete a un nodo, cuyo origen es el host A, provoca el envío de un paquete de restricción debido a que se ha superado el umbral de utilización y en el siguiente instante de monitorización llega un paquete procedente del host B. a) Se enviará de nuevo un paquete de restricción al host A. Indiana de proposicione de la companya de la compan b) El nodo enviará un paquete de restricción al host B. ... a sa sala a c) El nodo no enviará más paquetes de restricción hasta que no expire el temporizador que ha activado tras enviar el primer paquete de restricción. d) No tenemos suficiente información para saber si se envía o no el paquete de restricción al host B. d'depende de si llega par el mismo enlaa 14.- ¿Qué técnica de difusión genera menos carga en la red? Ya que u se calcula para a) Paquetes multidestino. cada enlace. b) Spanning tree o árbol de difusión. c) Spanning tree adaptativo o dinámico. d) Inundación. 15.- Una red con estructura jerárquica está formada por N niveles. El primer nivel de la jerarquía consiste en N agrupaciones de N nodos. Los N-1 niveles restantes están formados por N agrupaciones del nivel inmediatamente inferior. ¿Cuántas entradas aparecen en la tabla de cada nodo? a) N! b) (N+1) x (N-1) c) N! x (N-1) b en cada d) Ninguna de las respuestas anteriores es correcta. bolita rulkimo nive 16.- Una de las diferencias de las redes con estructura interna tipo datagrama respecto a las hay 3 hosts redes con estructura interna tipo circuito virtual es que: a) En las redes circuito virtual la secuencia de salida de los nodos intermedios sigue siempre un patrón fijo mientras que en las redes tipo datagrama se realiza una multiplexación estadística. b) A diferencia de las redes tipo datagrama, en las redes tipo circuito virtual no se puede llegar a una situación de congestión. A diferencia de las redes tipo circuito virtual, en las redes tipo datagrama cada paquete se transmite a una tasa igual al total del ancho de banda del enlace. d d) Ninguna de las respuestas anteriores es correcta. 17.- A una interfaz de red se le ha asignado la dirección IP 162.35.24.52/28. ¿Cúal de las siguientes opciones es una dirección válida para otra interfaz de red de la misma subred? clase B + subred a) 162.35.24.34/28 162 = 10100010 728 bik = red + subred 35 = 00 10 0011 24 = 0001 1000 52 = 0011 0100 b) 162.35.24.47/28 c) 162.35.24.61/28 00110000 d) Ninguna de las respuestas anteriores es correcta. lasubred es 162.35.24.48

162. 35. 24. 49 - 162. 35. 24. 62

broadcast 162.35.24.63

04110001

18.- ¿Cuál es la dirección de broadcast de la subred de la cuestión anterior? a) 162.35.255.255 b) 162.35.24.255 and is resolve the literature of profit and automorphic of the literature of the lite (c) 162.35.24.240 For the about the land the state of the d) Ninguna de las respuestas anteriores es correcta. 19.- ARP: a) Se utiliza en redes de difusión. b) Dada una dirección física (MAC) conocida de una máquina, se puede utilizar para obtener la dirección IP de dicha máquina. c) Al igual que ICMP se encapsula en datagramas IP. d) Ninguna de las respuestas anteriores es correcta. 20.- La arquitectura de protocolos Aplicación/UDP/IP/Frame Relay: a) Debido a Frame Relay es necesario que en vez de UDP se utilice TCP.
b) La recuperación de errores se realiza en la capa más alta. c) IP es innecesario porque Frame Relay es ya capa de red. - cierto, pero UDP sólo sabe funcionar solore IP d) Es equivalente a otra arquitectura en la que en vez de UDP se utilice ICMP.

a

CUESTIONES Y PROBLEMAS (6 puntos)

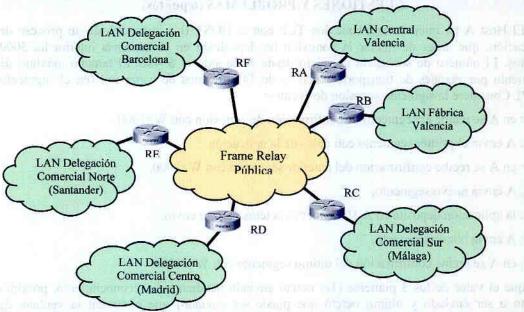
- 1.- El Host A ha iniciado una conexión TCP con el HOST B a instancias de un proceso de aplicación, que antes de iniciar la conexión ha depositado en la memoria intermedia 3000 octetos. El número de secuencia de inicio desde A ha sido el 65432. El tamaño máximo de segmento por razones de transporte físico es de 1460 octetos de carga útil (en el segmento TCP). Considere la siguiente sucesión de eventos:
- T1: en A se recibe el segmento de confirmación de conexión con W=1000,
- T2: A envía el primer segmento con datos de la aplicación,
- T3: en A se recibe confirmación del anterior segmento con W=2000,
- T4: A envía nuevo segmento,
- T5: la aplicación deposita en A 1000 nuevos octetos para su envío,
- T6: A envía nuevo segmento,
- T7: en A se recibe confirmación del último segmento con W=3000

Indique el valor de los 3 punteros (1er octeto enviado pendiente de reconocimiento, próximo octeto a ser enviado y último octeto que puede ser enviado) que controlan la ventana de transmisión del Host A inmediatamente después de los instantes temporales indicados:

MeU	V.Dr.Plantie	P2 P2	пр прито РЗ) за зар
T1		dis ent miter the 2 suit	abidos en cada man
T2	C TO THE TOTAL	promise and	ada de conexionado
T3	SUPPLIE ARION OF	तिवस्ति तेल कि तद्यों भारत	Significant se dendi
T4	5011		
T5	A35		
T6			7985
T7		1600	

(2 puntos)

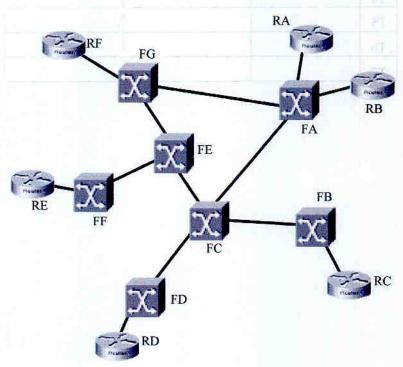
2.- En la figura siguiente se representa la solución de la red de comunicación de datos de una empresa valenciana.



Como puede apreciarse tanto la sede central, como en la fábrica y en las delegaciones comerciales existen sendas redes de área local, con arquitectura TCP/IP, todas ellas conectadas a una red pública Frame Relay que posibilita su interconexión.

Interconexión que se concreta en un conjunto de circuitos virtuales (C.V.) permanentes (modo simplex) contratados en cada interfaz, y que unen los distintos "routers" que dan acceso a cada una de las redes de área local mediante tunnelling a través de los CV, configurando una topología mallada de conexionado.

En la figura siguiente se detalla parte de la red Frame Relay, destacando los nodos que gestionan los circuitos virtuales que nos interesan, así como los enlaces físicos que unen dichos nodos.



La red corporativa tiene una conexión a la red Internet a través de 2 circuitos virtuales permanentes adicionales (uno de entrada y otro de salida), desde la sede central de la empresa en Valencia hasta el nodo FC de la red Frame Relay Pública donde se realiza la conexión a un nodo (router) de Internet.

a) A partir de la información de las tablas de encaminamiento de circuito virtual simplex con relación a las conexiones que nos interesan, determine razonadamente la topología lógica de interconexión de las LAN (malla formada por los routers de acceso y los túneles a través de los circuitos virtuales permanentes contratados).

Ent.		Sal.	
RA	1	RB	1
RB	1	RA	1
RA	2	FC	1
FC	1	RA	2
RA	3	FG	1
FG	1	RA	3
RA	4	FC	2
FC	2	RA	4
RB	2	FC	3
FC	3	RB	2
RB	3	FG	2
FG	2	RB	3

Ent.		Sal.	
FC	1	RC	1
RC	1	FC	1

Sal.

RD

RE

FE

Nodo FD Ent.

FC

FE RE

Ent.		Sal.	
FA	. 1	FD	1
FD	1	FA	1
FA	2	Inter	net
Inter	net	FA	2
FD	2	FB	1
FB	1	FD	2
FA	3	FD	3
FD	3	FA	3

Nodo	FE		
Ent.		Sal.	
FG	1	FF	1
FF	1	FG	1

RD	1.4	FC	1	
RD	2	FC	2	
FC	2	RD	2	
FC	3	RD	3	
RD	3	FC	3	

Ent.		Sal.	
FA	1	RF	1
RF	1	FA	1
RF	2	FE	1
FE	1	RF	2
FA	2	RF	3
RF	3	FA	2

Matrice

Surface

1 panel

3 - Sur in milh do in figure con her cases de les dispinçe unia de la case un protecule de convolute enconfigue con la passe un case de la case de la

b) Si cada C.V. contratado: III la presente los el muneros muneros del asistempos del ad-

Intervalo comprome	de tida (T	medida	de	velocidad	1 segundo
CBS (CIR*	*T)	amusi wa	ni spi	otimizai 30s	100 bits
EBS (EIR*	T)	F. ALIRY DE			25 bits

Sabiendo que:

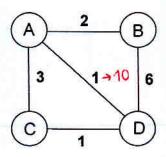
- las velocidades de línea (full-duplex) posibles son: 2ⁿ*64 kbps, n=1..6,
- las velocidades de línea contratadas en cada interfaz deben ser lo más pequeñas posibles,
- cada interfaz con la red Frame Relay debe cubrir las necesidades conjuntas de los C.V. de cada interfaz, tanto de velocidad comprometida como de ráfaga en exceso,
- y que la suma de CIR y EIR globales en cada interfaz no puede exceder del 75% de la velocidad de línea.

Complete la tabla correspondiente a la descripción de cada interfaz Frame Relay contratada.

1 87	Cantidad de C.V. entrada/salida	CIR global necesario	EIR global necesario	Velocidad de línea contratada
Central-Valencia	3.9		No.	III obol
Fábrica- Valencia	LAT.	192		73 1 08
Barcelona	DE I			
Madrid				
Málaga				
Santander				

(1 punto)

3.- Sea la malla de la figura con los costes de los distintos enlaces. En ella opera un protocolo de control de encaminamiento de Vector Distancia con horizonte dividido y retorno envenenado. Fruto de la evolución del protocolo son las tablas de encaminamiento que se adjuntan. Indique la evolución de dichas tablas si el coste del enlace directo entre A y D pasa a ser 10. Considere que los nodos A y D se dan cuenta simultáneamente del cambio, y que los tiempos de proceso en cada nodo, así como de intercambio de información a los vecinos, son iguales en todos los casos.



DA	В	C	D	$\mathbf{D_B}$	A	D	De	A	D	$\mathbf{D}^{\mathbf{D}}$	A	В	С
В	2	7	00	A	2	7	A	3	2	A	1	8	
C	∞	3	2	C	4	7	В	5	4	В	3	6	00
D	∞	4	①	D	3	6	D	4	1	С	œ	10	1
VD	B (2) 7 00 (3) 00 (4)	00) 11) 10]	(c-3,	A (2) C D (3)	D F (F (6		D° A B D	3 5 4 (7 C1	10 (8 12 (€ ∞ 1	0 (1)	
AD _b	, bou	LD	(c-:	D-∞ <i>)</i>				V	D ^D par	ra A (B a B (F a C (F	1-∞ 1-8,) B-6)
DA	B (2) 7 (2) 8 (4)	D 16	Z Maja	D A (25)	D 7 8 7 6		D'ABD	A 3008	D 7 7 1	A	A B 10 8 12 6 13 10	000	
^	ada	200		Į				1					
			ADB b	ora D (Co ora D (Co	- 6] - 6])-6))-)	1 Dc - 1 Dc 1 Dc	bar bar bar	aA(aB(aD(8-00) N-8) H-3, B-	- no 1	o rec	logia ivia cinos
DIBCD	8 8 8	2 D 2 16 3 11 3 10		A D G	D 76		De	A B B C C	D	D	A B 0 8 1 12 (6) 13 11	C	
C	ada			naďe			N	بعر	/D ^D pa	sa A - r ia B (A ra C (A	1 (ads (-4)	\ \ \	
DA B 2 C 0 8	C 1839) 6 1		DB A 000 D 600 D 600	D 10 7		D _C	A GGG &	D	D	A B	C	
			Ta	blas o	pti	mas							
32 N	22												

(2 puntos)