Traffic Analysis

- Introducción -

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Programa de Tecnologías para la gestión distribuida
de la información

Contenido

- Ejemplos introductorios
- Terminología y modelos
- Captura de tráfico
- Artículos

Ejemplos introductorios

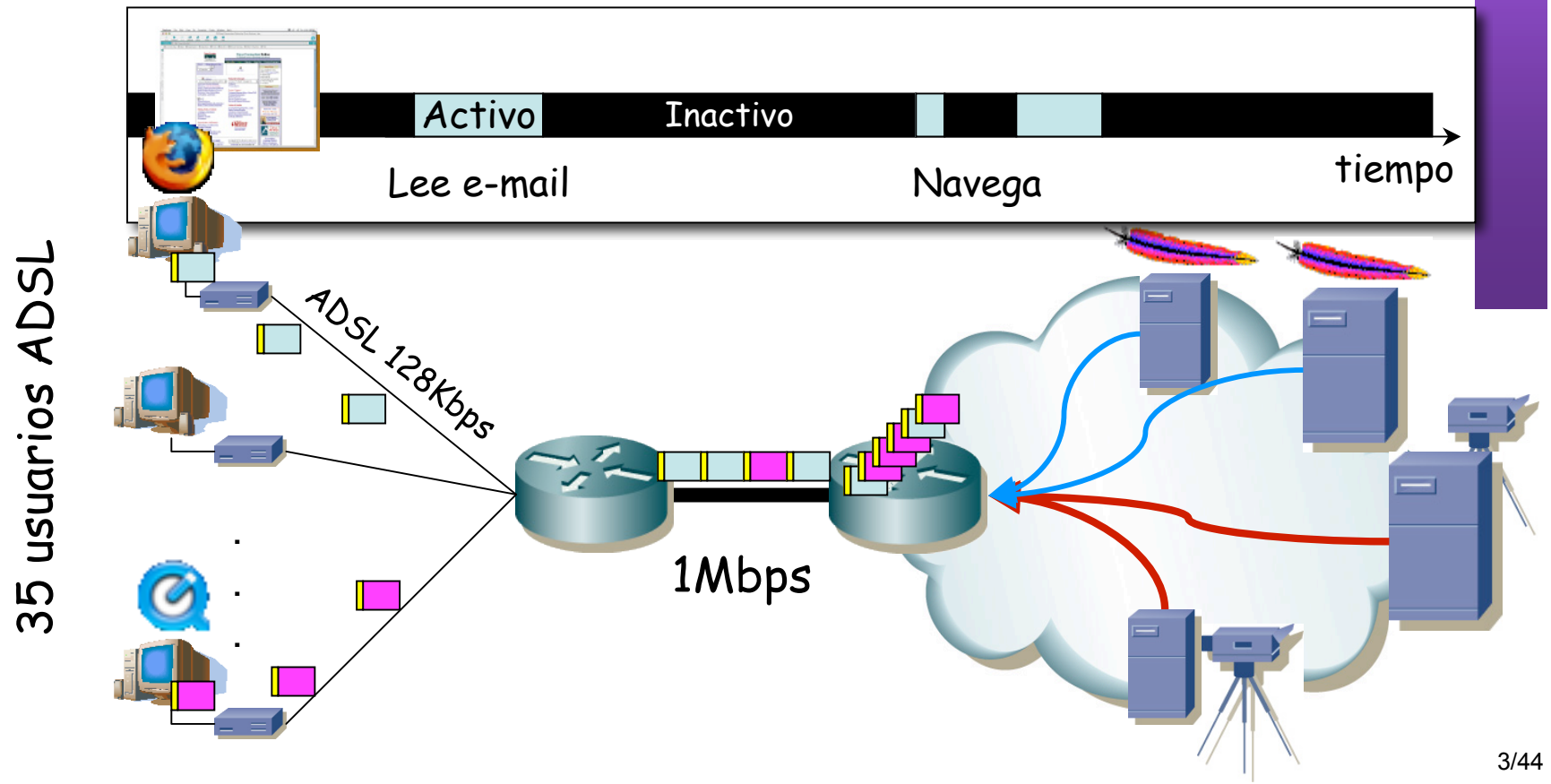
Ejemplo de red

Cada usuario:

- Recibe de un servidor a 100Kbps cuando está activo
- Activo cada uno un 10% del tiempo

10 usuarios a 100Kbps=1Mbps

¿ Cuál es la probabilidad de que más de 10 usuarios reciban tráfico a la vez ?



Ejemplo de red

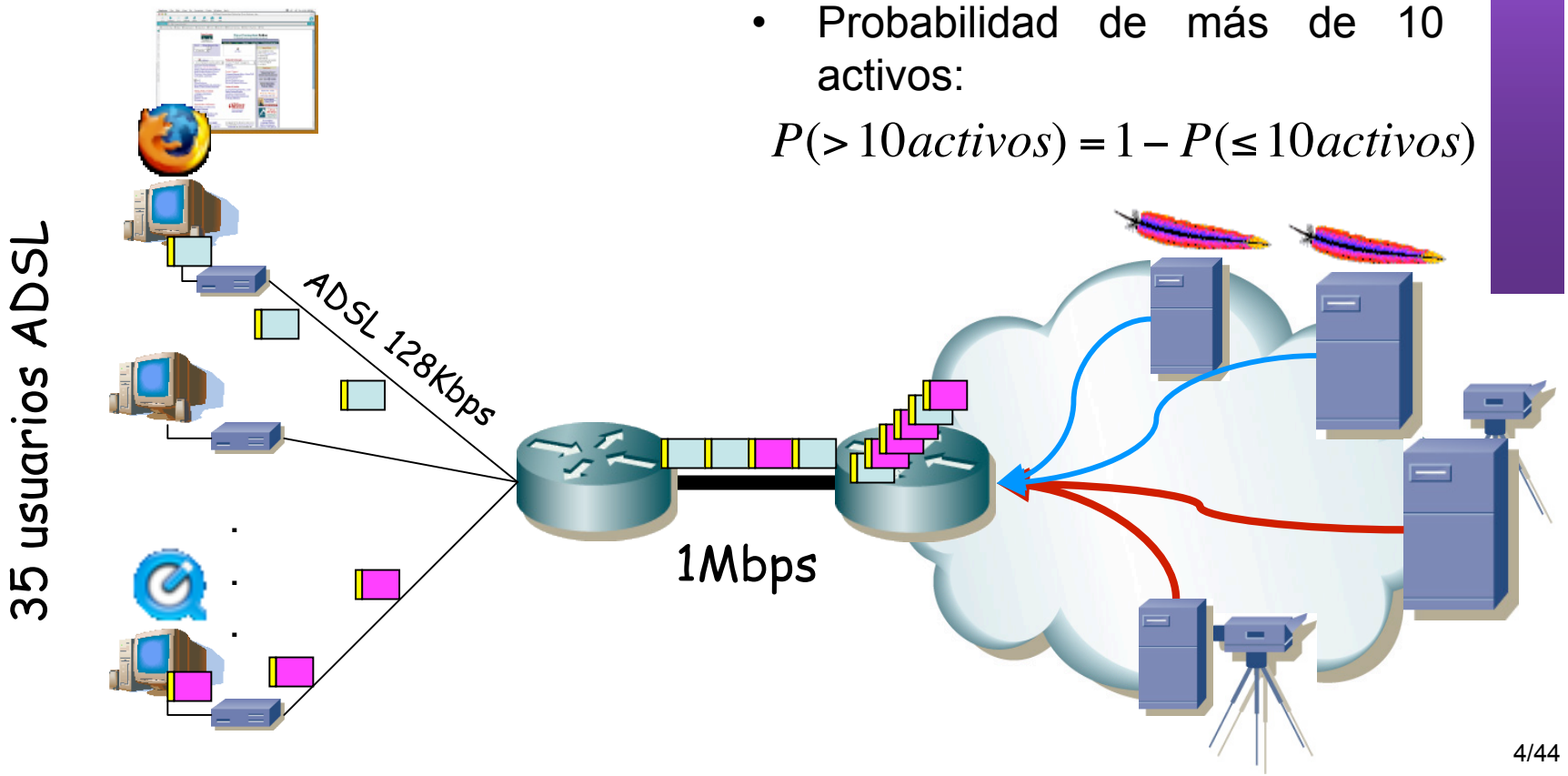
¿ Cuál es la probabilidad de que más de 10 usuarios reciban tráfico a la vez ?

- Usuario activo un 10% del tiempo
- Supongamos pues que en un momento cualquiera:

$$P(usuario\_activo) = 0.1 = p$$

- Probabilidad de más de 10 activos:

$$P(>10 activos) = 1 - P(\leq 10 activos)$$

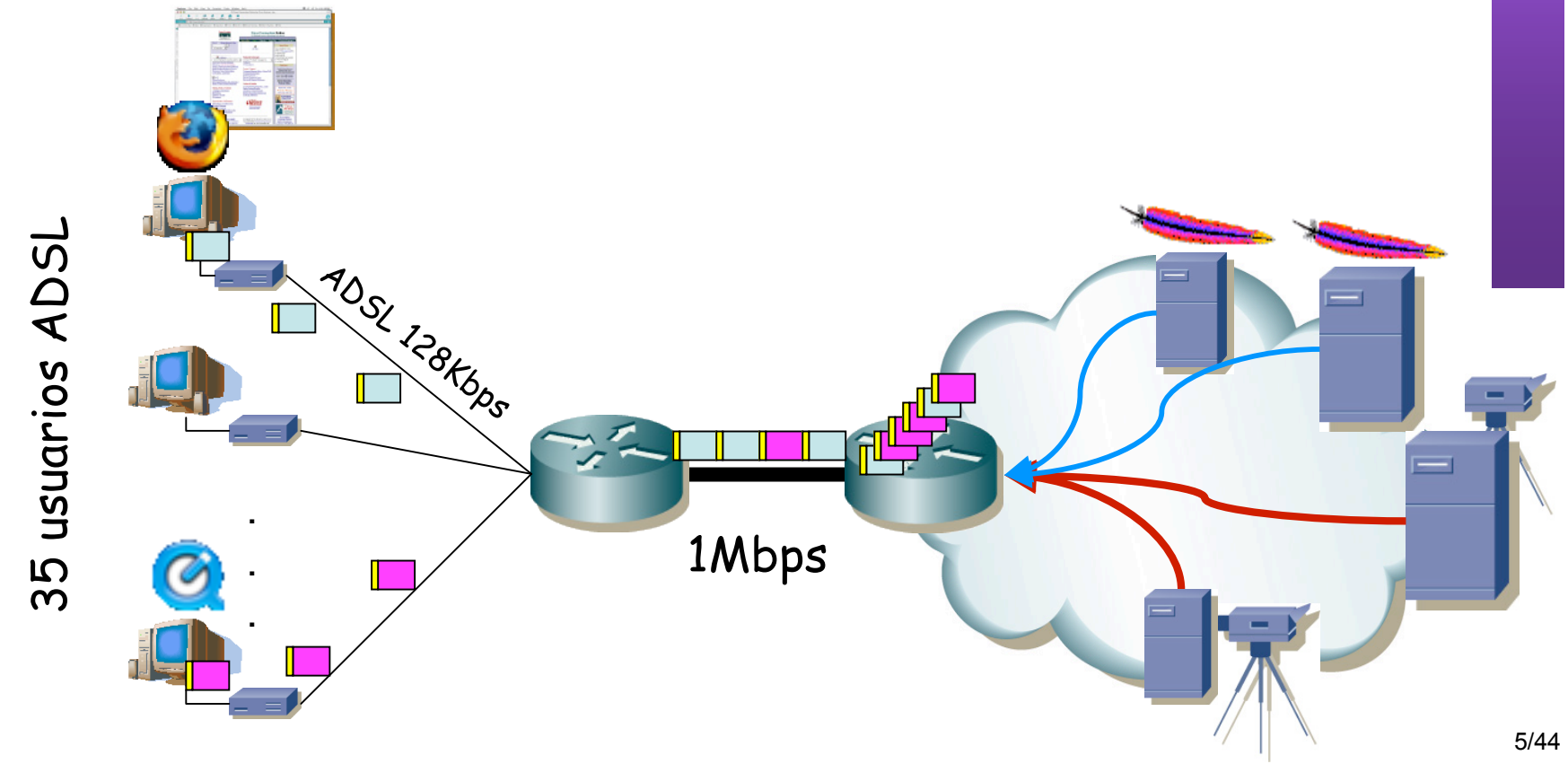


Ejemplo de red

¿ Cuál es la probabilidad de que más de 10 usuarios reciban tráfico a la vez ?

$$P(>10 activos) = 1 - P(\leq 10 activos)$$

$$P(\leq 10 activos) = P(0\_activos) + P(1\_activo) + \ldots + P(10\_activos) = \sum_{i=0}^{10} P(i\_activos)$$



Ejemplo de red

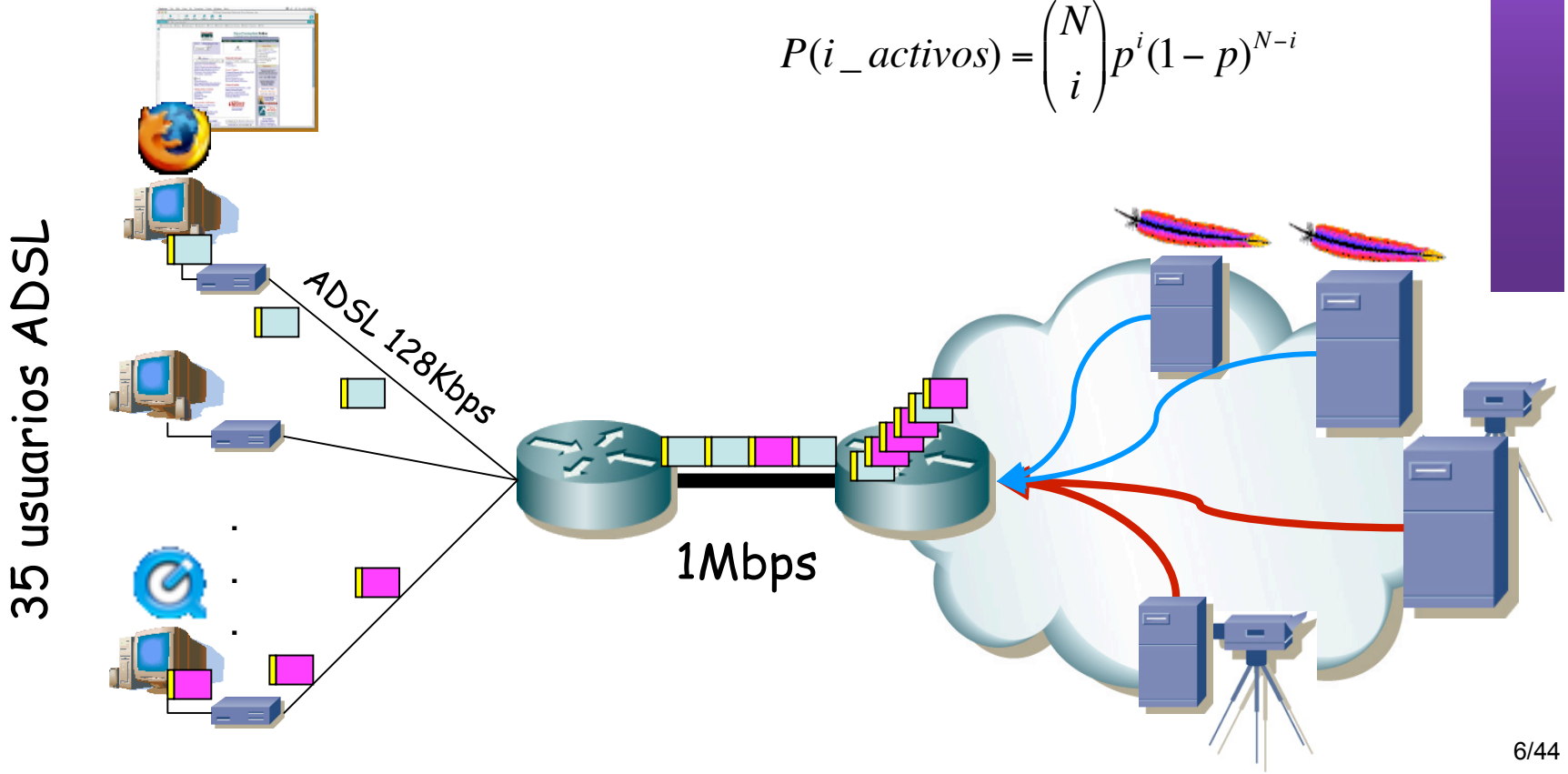
¿ Cuál es la probabilidad de que más de 10 usuarios reciban tráfico a la vez ?

$$P(0\_activos) = (1-p)^N$$

$$P(1\_activo) = Np(1-p)^{N-1}$$

$$P(2\_activos) = \frac{N(N-1)}{2} p^2(1-p)^{N-2}$$

$$P(i\_activos) = \binom{N}{i} p^i(1-p)^{N-i}$$



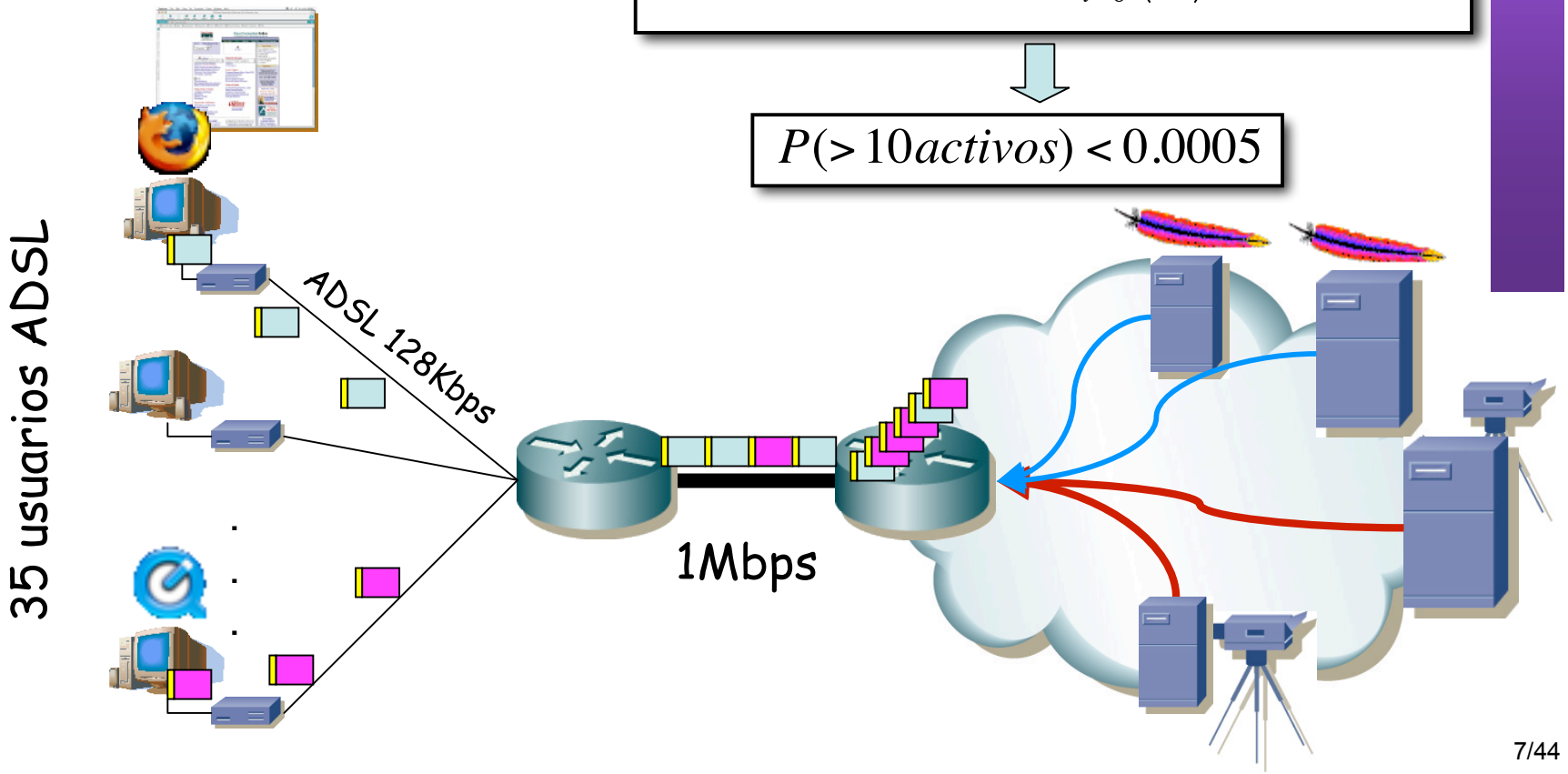
Ejemplo de red

¿ Cuál es la probabilidad de que más de 10 usuarios reciban tráfico a la vez ?

$$P(\leq 10 activos) = \sum_{i=0}^{10} \binom{N}{i} p^i (1-p)^{N-i}$$

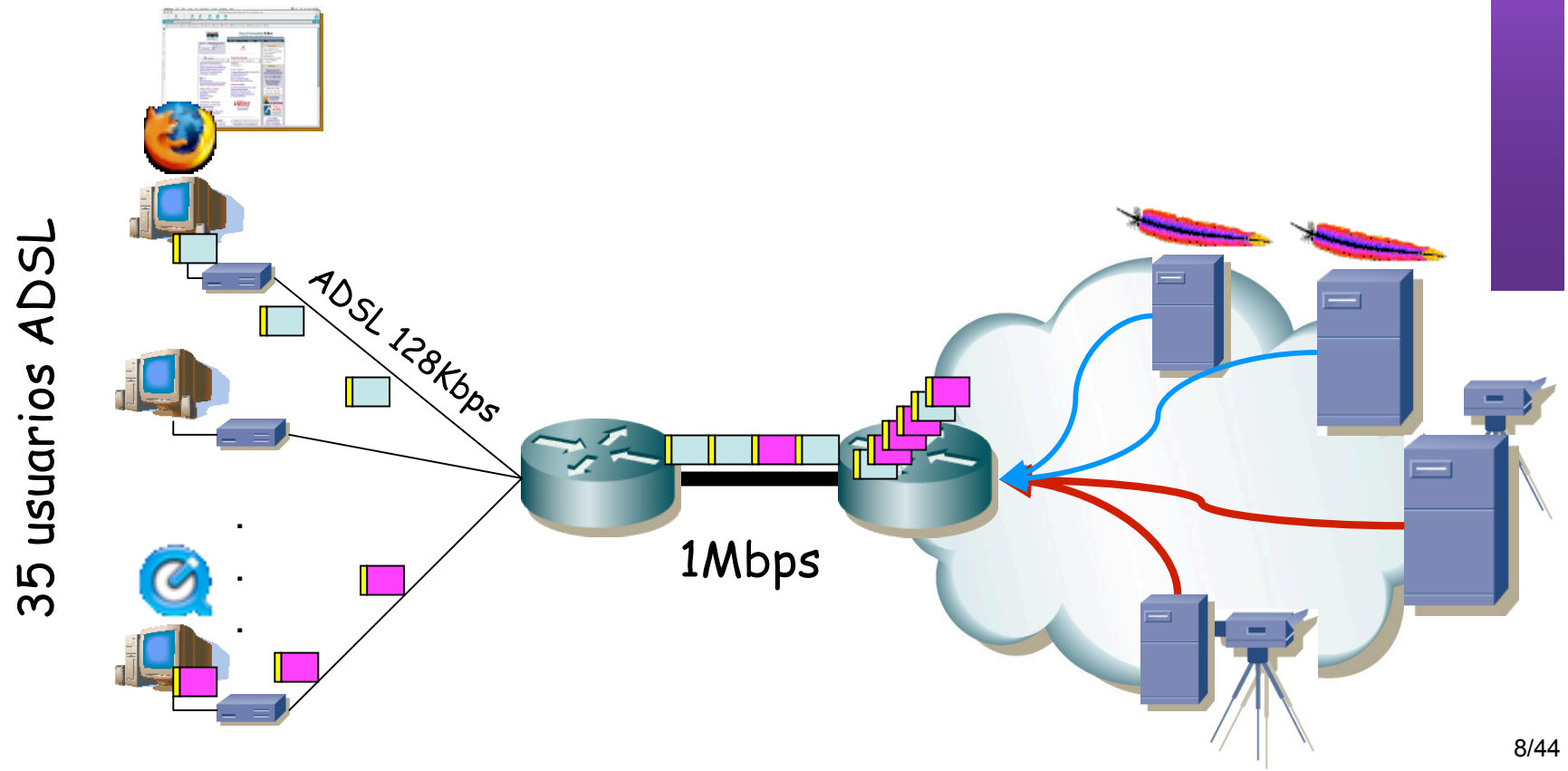
$$P(> 10 activos) = 1 - \sum_{i=0}^{10} \binom{N}{i} p^i (1-p)^{N-i}$$

$$P(> 10 activos) < 0.0005$$



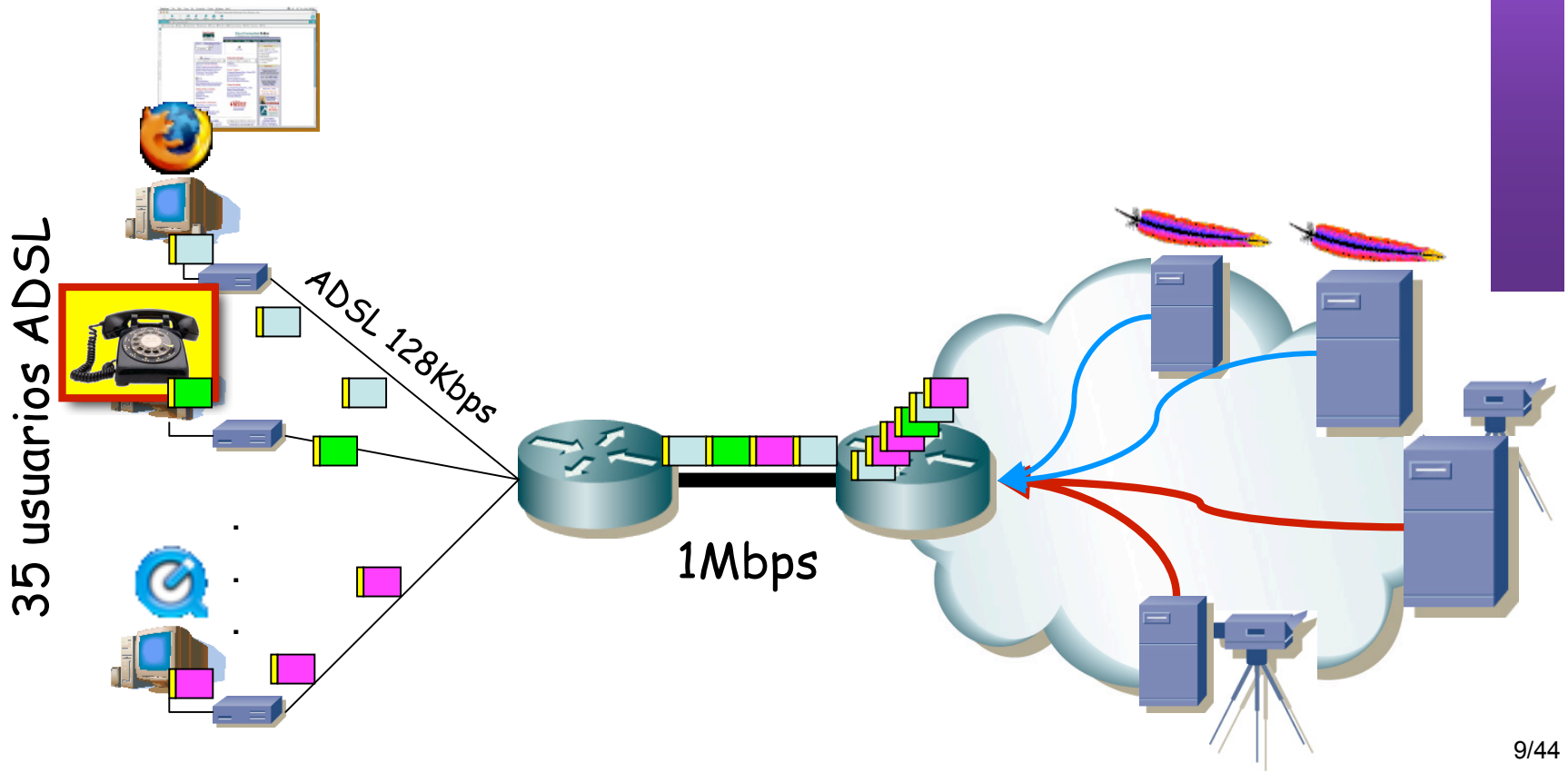
Ejemplo de red

- 35 usuarios x 128 Kbps/usuario = 4,48Mbps
- 4,48Mbps > 1Mbps
- Congestión en enlace de acceso sin dar 128Kbps a todos los usuarios
- *Sobresuscripción* (overbooking)



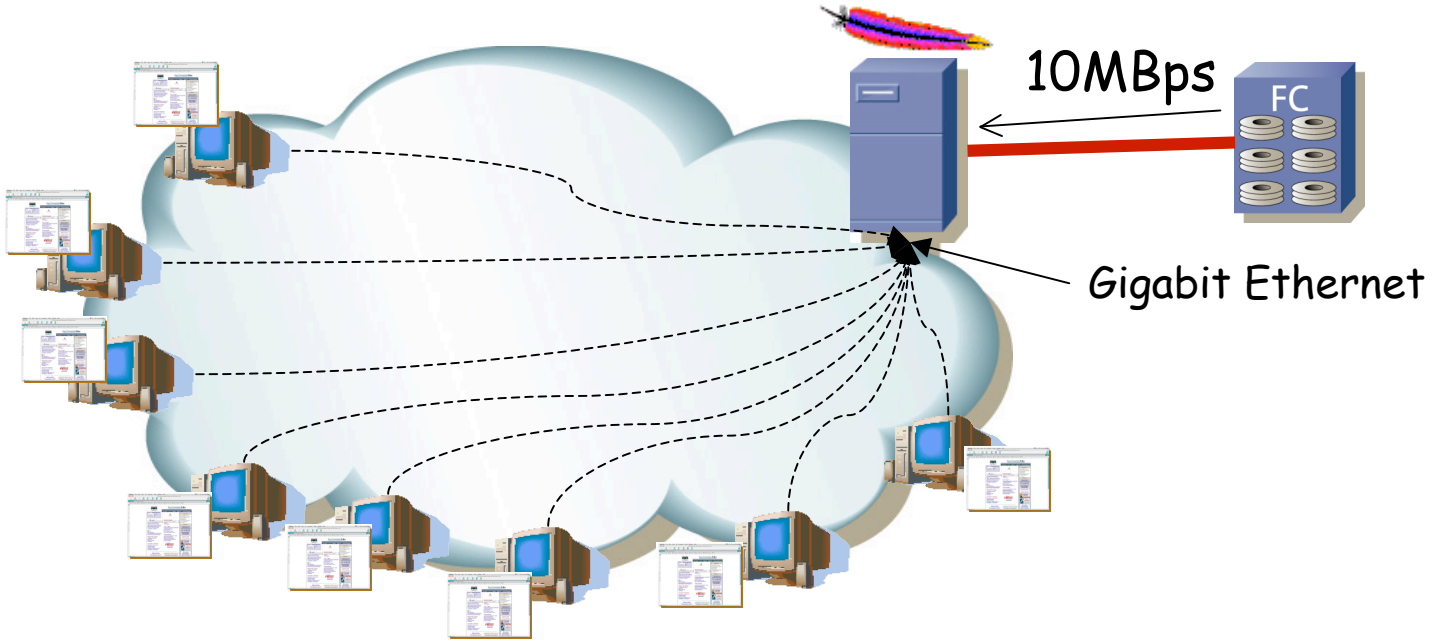
Ejemplo de red

- Si ahora un usuario quiere emplear una aplicación de voz
- Pérdidas
- Excesivo retardo



Ejemplo de aplicación

- Peticiones a un servidor web
- 1.000 peticiones por segundo ⇒ nueva petición cada 0,001 segs
- Tamaños de los ficheros 100KBytes
- Discos sirven a 10MBps (80Mbps) ⇒ 1 fichero servido en 0,01 seg ⇒ 100 ficheros servidos por segundo
- ¡ Hay 10 veces más peticiones por segundo que las que soportan los discos !

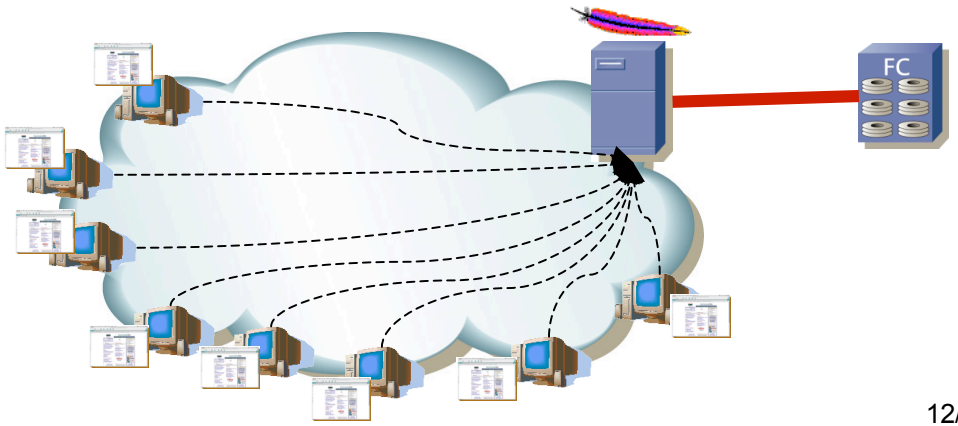


Terminología y modelos

Terminología

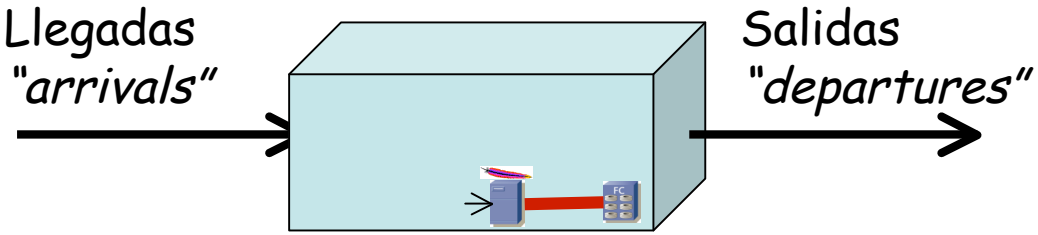
- Peticiones recibidas: *"Tasa de llegadas"* = *"Arrival rate"* = λ (1.000 peticiones/seg)
- Hemos supuesto que cada 0,001 segs una nueva: llegadas *Deterministas*
- Los discos sirven a 80Mbps
- Los tamaños de los ficheros son constantes (100KBps)
- *Capacidad del servidor:* Velocidad/Tamaños = 100 peticiones/seg = μ
- El sistema es estable si y solo si:

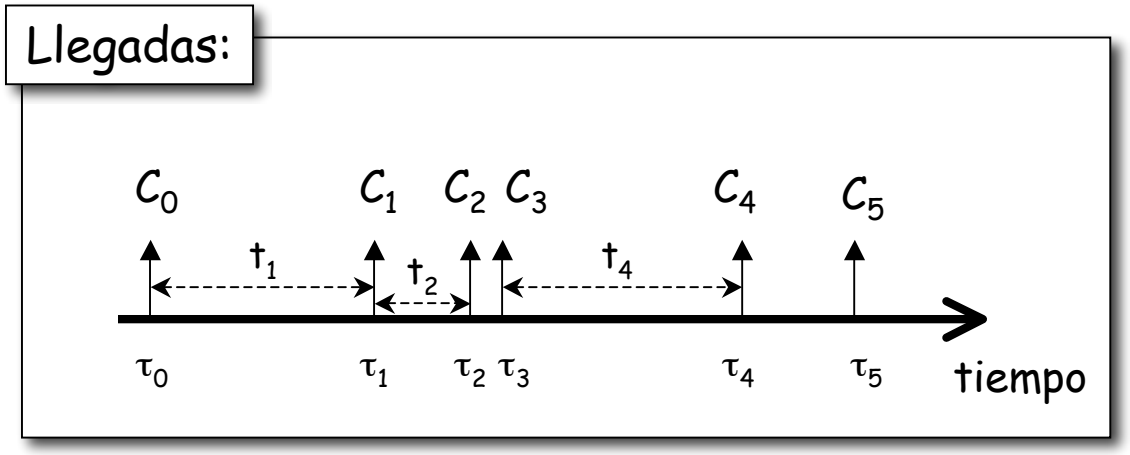
  Tasa de llegadas < *Capacidad del servidor* ($\lambda<\mu$)

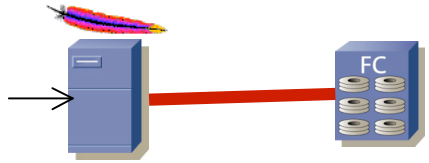


Terminología

- $\mathbf{C_n}$: Llegada n-ésima
- $\boldsymbol{\tau_n}$: instante de la llegada C_n
- $\mathbf{t_n}$: tiempo entre la llegada C_{n-1} y la C_n ($\mathbf{t_n = \tau_n - \tau_{n-1}}$)
- x_n : tiempo de servicio de la llegada C_n



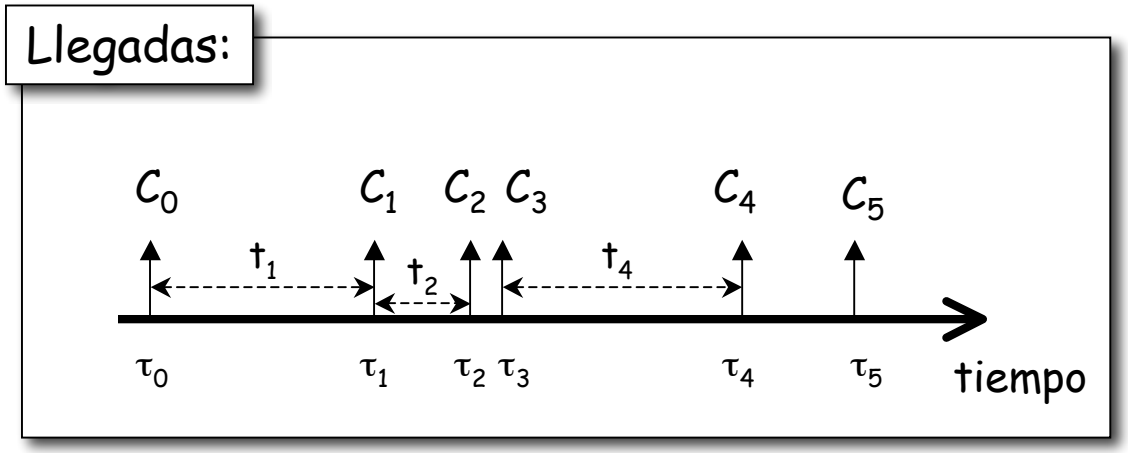


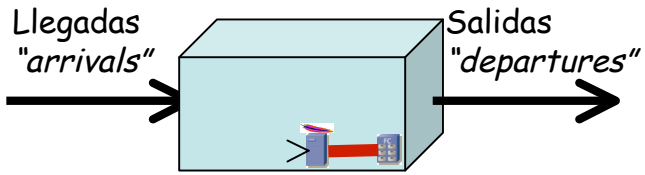


Aleatoriedad en las llegadas

- Generalmente los instantes de llegada serán aleatorios
- Cada $\mathbf{t_n}$ es una variable aleatoria
- Suposiciones más habituales (i.i.d.)
  - Todas las vv.aa. $\mathbf{t_n}$ siguen la misma distribución $\underline{\mathbf{t}}$
  - Todas las $\mathbf{t_n}$ son vv.aa. independientes
- **A**(t) función de distribución del tiempo entre llegadas:

  A(t) = P(tiempo entre llegadas ≤ t)

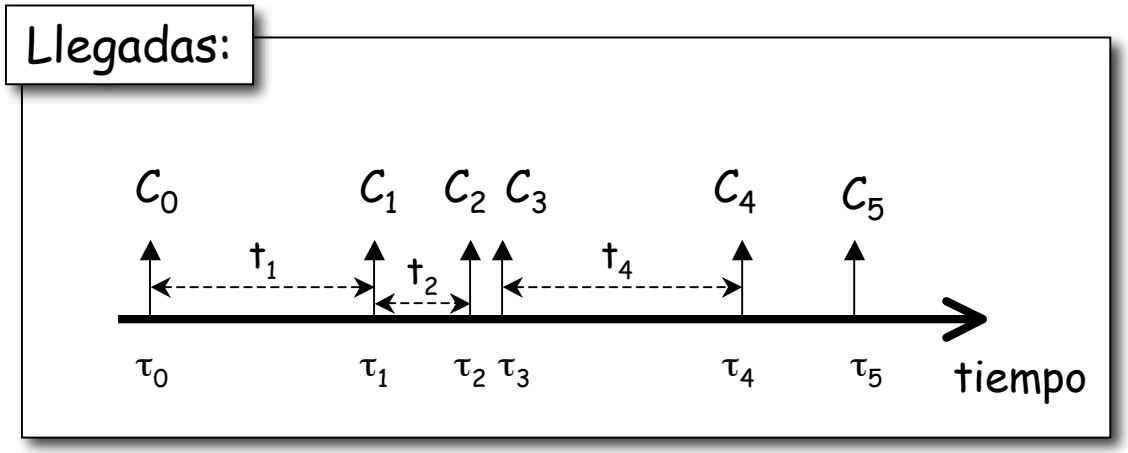


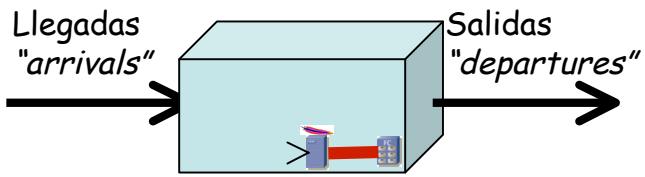


Aleatoriedad en los servicios

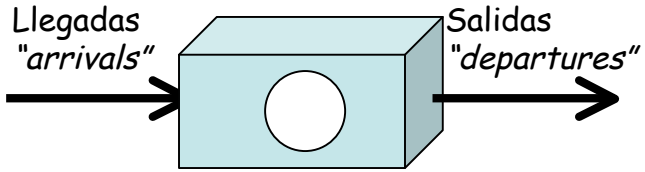
- Generalmente las duraciones de los servicios serán aleatorias
- Cada $\mathbf{x_n}$ es una variable aleatoria
- Suposiciones más habituales (i.i.d.)
  - Todas las vv.aa. $\mathbf{x_n}$ siguen la misma distribución $\underline{\mathbf{x}}$
  - Todas las $\mathbf{x_n}$ son vv.aa. Independientes
- **B**(x) función de distribución del tiempo entre llegadas:

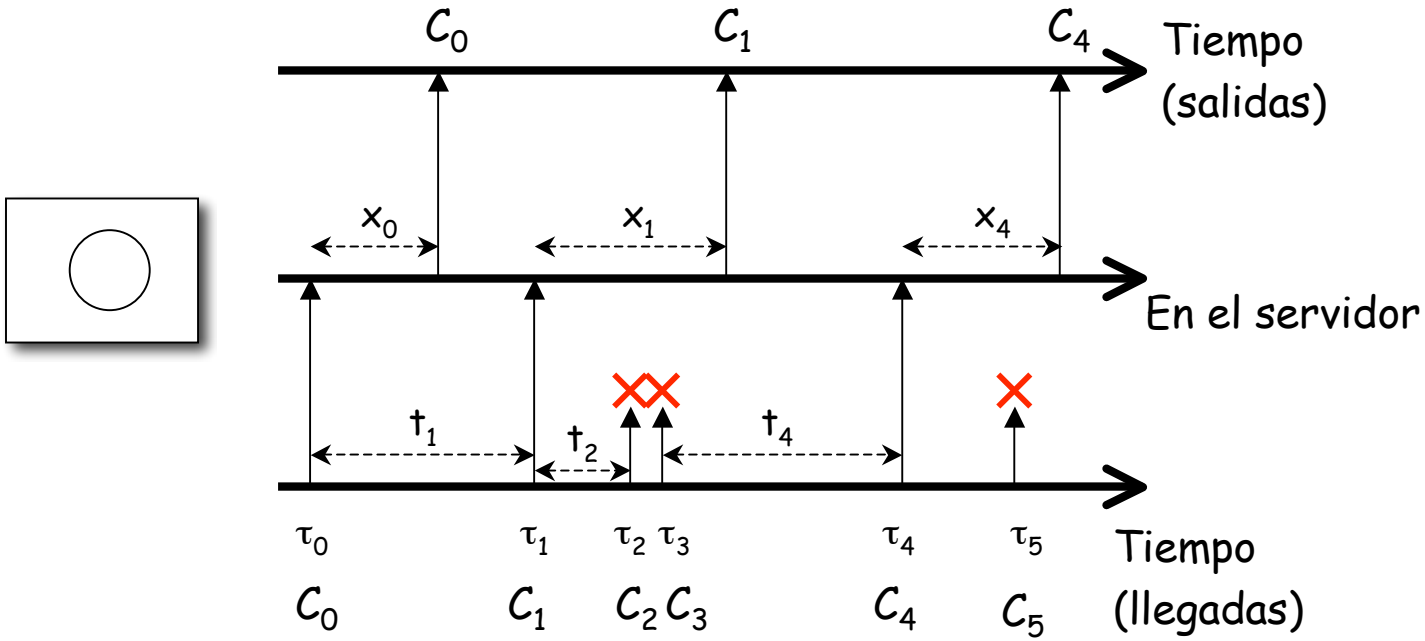
  B(x) = P(tiempo de servicio ≤ x)





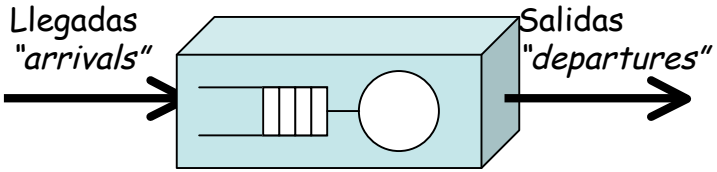
Pérdidas

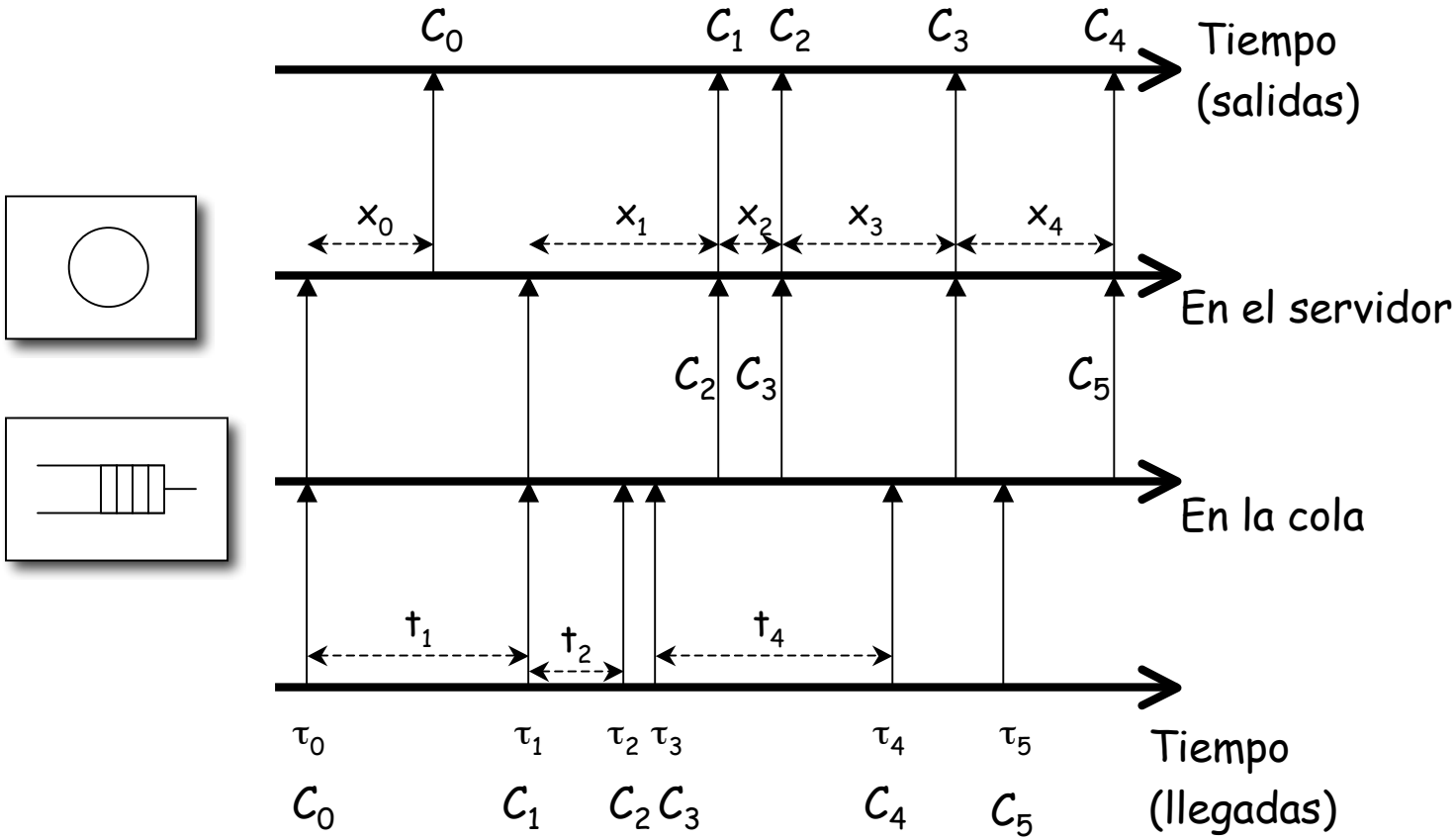

Llegadas
"arrivals"
Salidas
"departures"


C_0
C_1
C_4
Tiempo
(salidas)
x_0
x_1
x_4
En el servidor
t_1
t_2
t_4
τ_0
τ_1
τ_2 τ_3
τ_4
τ_5
Tiempo
(llegadas)
C_0
C_1
C_2 C_3
C_4
C_5

Con cola

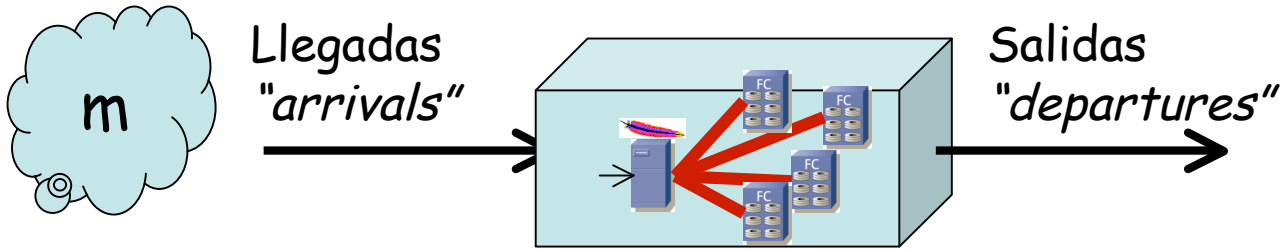
- Cola infinita o con tamaño máximo





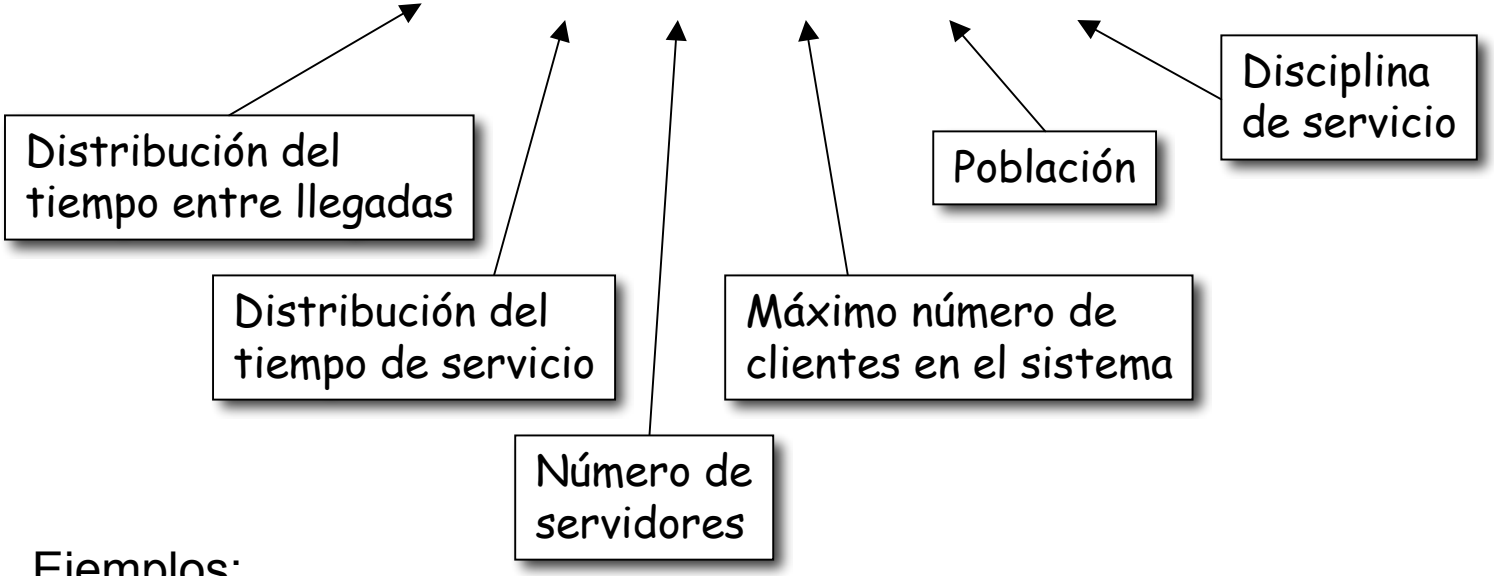
Otros parámetros

- El número de servidores puede ser distinto de 1
  - ¿Todos sirven de igual manera? (misma distribución del tiempo de servicio)
  - ¿Cómo se selecciona servidor?
- Número máximo de clientes que puede haber en el sistema
- Número máximo de clientes *"en el universo"* (m)
- ¿FIFO? ¿LIFO? ¿Prioridades? ¿Según tamaño? ¿Al azar? ¿Preemptivo?



Notación de Kendall

A / B / c / K / m / Z



- Ejemplos:
  - *"M"* : distribución exponencial : $P(X < x) = 1 - e^{-\beta x}$
  - *"D"* : determinista
  - *"G"* : distribución genérica

  - *"M/M/1"* : tiempos entre llegadas exponenciales, tiempos de servicio exponenciales, 1 solo servidor
  - *"D/D/2/5"* : tiempos entre llegadas deterministas, tiempos de servicio deterministas, 2 servidores, máximo de 3 clientes en cola

¿Podemos resolverlos?

- Podemos querer calcular:
  - Tiempo entre una llegada y que se completa su servicio:
    - Tiempo medio, distribución…
    - Nos sirve para saber si el sistema da un servicio de “suficiente” calidad
  - Número de peticiones encoladas ante una nueva llegada
    - Número medio, distribución…
    - Nos ayuda a saber cuánta cola deberíamos poner
  - Cómo son las salidas
    - ¿Siguen siendo deterministas/exponenciales/lo_que_sea?
    - Necesario conocerlo si detrás hay otro sistema que tome nuestros servicios como nuevas llegadas

- Podemos calcularlo:
  - Para algunos sistemas sencillos (D/D/c, M/M/c/K, etc)
  - Aproximaciones, cotas, para sistemas un poco más complejos
  - Simulación para sistemas “reales”

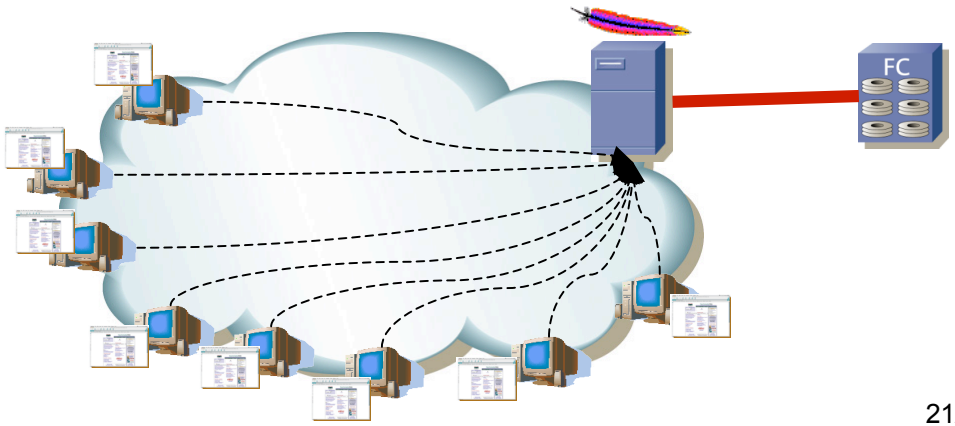
Ejemplo de aplicación

- Llegadas las tomamos equiespaciadas (determinista)
- Los tiempos de servicio siempre iguales (determinista)
- Los discos solo pueden servir 1 fichero a la vez

D/D/1

- ¿Cola? ¿Cuántas peticiones puede almacenar sin servir el servidor?
- Por ejemplo supongamos que es un servidor web multihilo que se bloquea el hilo al recibir una petición
- Tantos servidores como hilos (h)

D/D/1/h

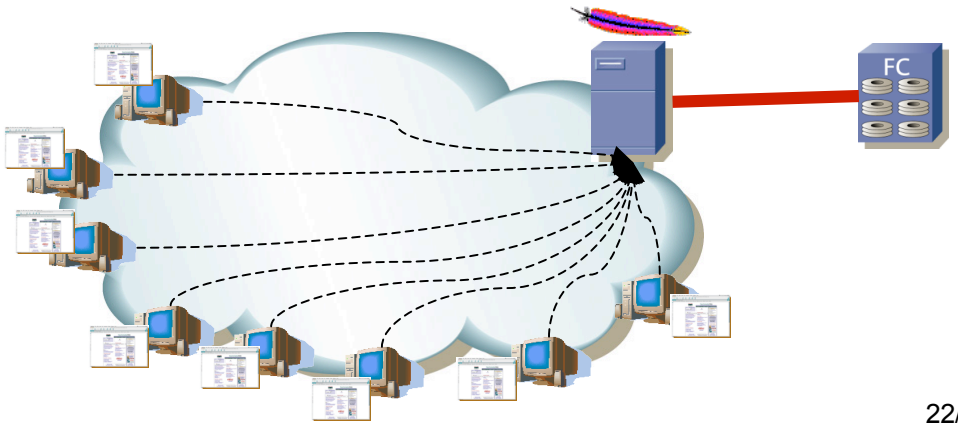


Ejemplo de aplicación

D/D/1/h

¿Son hipótesis realistas?

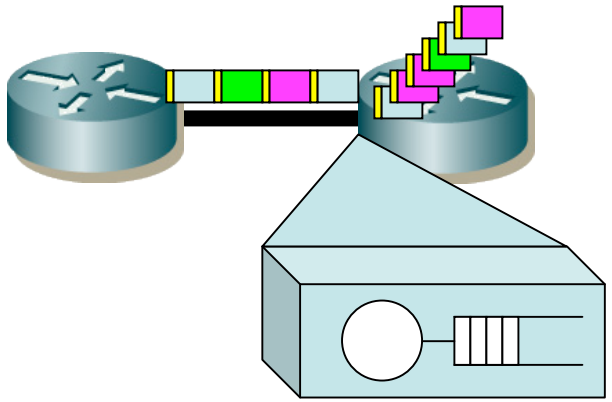
- No hace falta cola: si no es capaz de servir antes de la llegada siguiente ($\lambda > \mu$) el sistema será inestable
- Las llegadas serán normalmente aleatorias y dependerán principalmente del comportamiento de los usuarios
- Los tiempos de servicio dependen del tamaño de los ficheros y no son todos iguales
- También los tiempos dependerán de la red (ej. TCP)



Ejemplo de red

- Las llegadas son de los paquetes
- El tiempo de servicio es el tiempo de enviar el paquete
- El tiempo depende del tamaño del paquete
- La cola es el tamaño del buffer de memoria de paquetes

- ¿Cómo son los tiempos de llegada de paquetes a un router?
- ¿Cómo son los tamaños de los paquetes?
- ¿Es igual para cualquier router? (al menos el tipo de distribución)

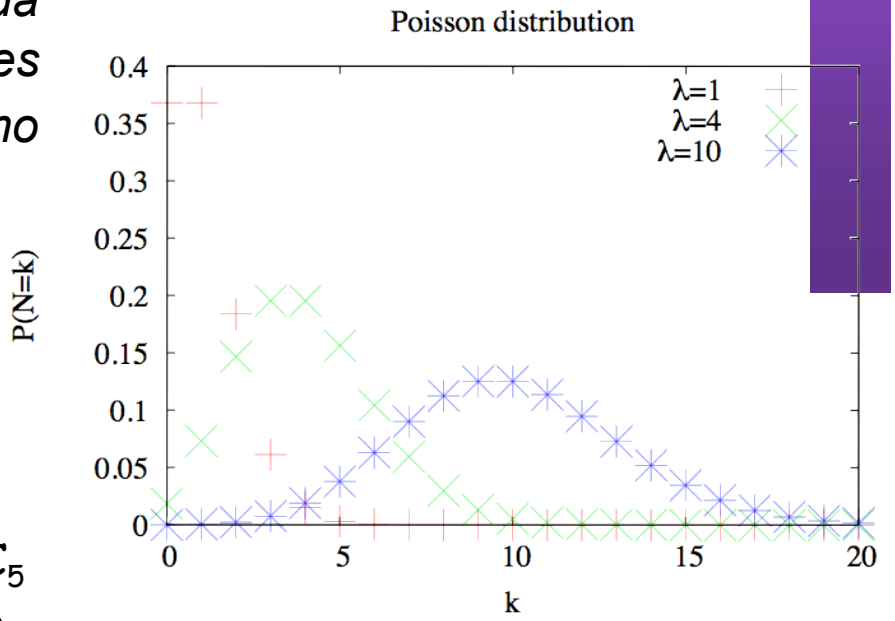


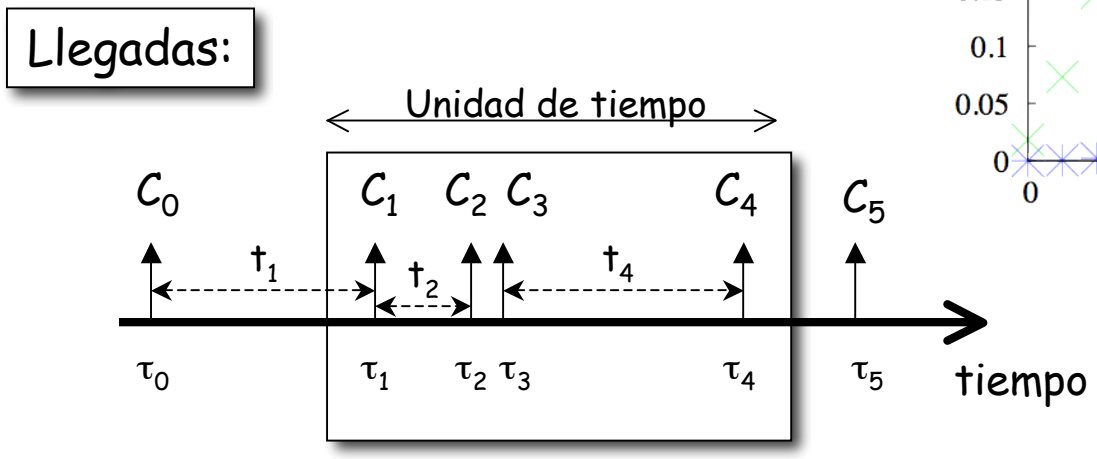
¿Con qué solemos trabajar?

Llegadas de *Poisson*

- El número de llegadas por unidad de tiempo sigue la distribución de *Poisson*
- Llegadas de peticiones de fichero, de paquetes, etc.
- $E[N] = \lambda$ llegadas/unidad de tiempo
- *La probabilidad de una nueva llegada en un intervalo incremental δ es proporcional a la duración del mismo ($\lambda\delta$)*

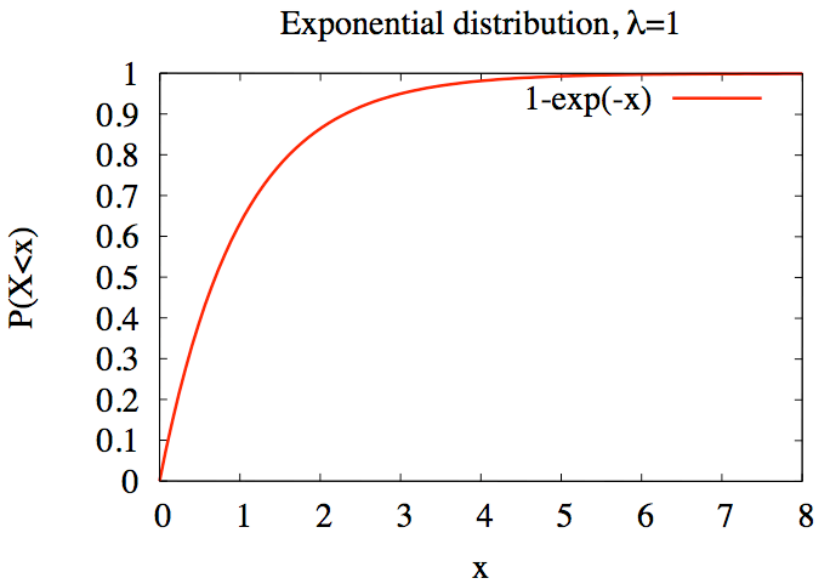
$$P(N = k) = \frac{\lambda^k}{k!} e^{-\lambda}$$

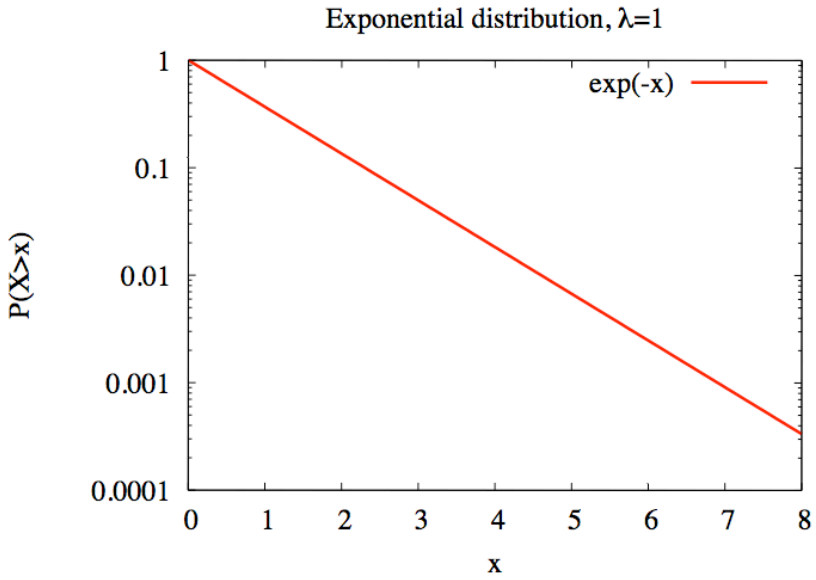




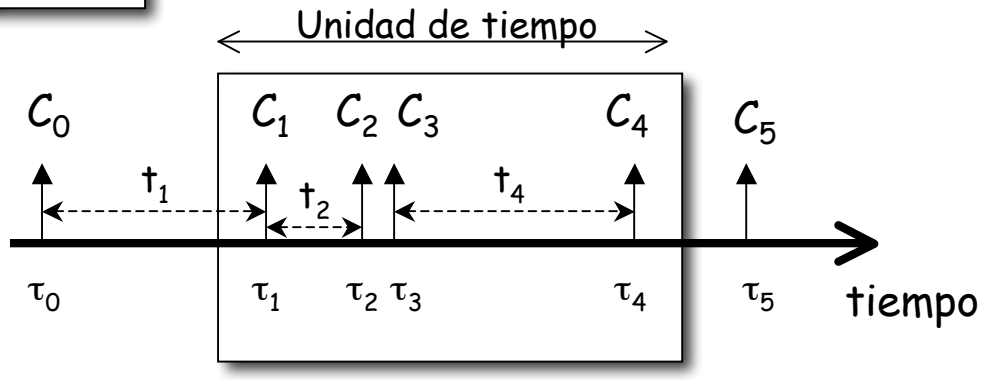
Llegadas de *Poisson*

- Los tiempos entre llegadas son i.i.d. y siguen una distribución exponencial (*M*)





Llegadas:



¿Llegadas de *Poisson?*

- ¿Los tiempos entre llegadas son i.i.d. y siguen una distribución exponencial (*M*)?
- ¿Equiespaciadas (determinista)?
  - Fuentes CBR
- ¿Los tiempos entre llegadas son independientes?
  - ¿Las peticiones de páginas web? El usuario suele navegar en "sesiones"
  - ¿Los paquetes IP? Si vienen varios paquetes suele haber bastante probabilidad de que vengan más ⇒ correlación no nula

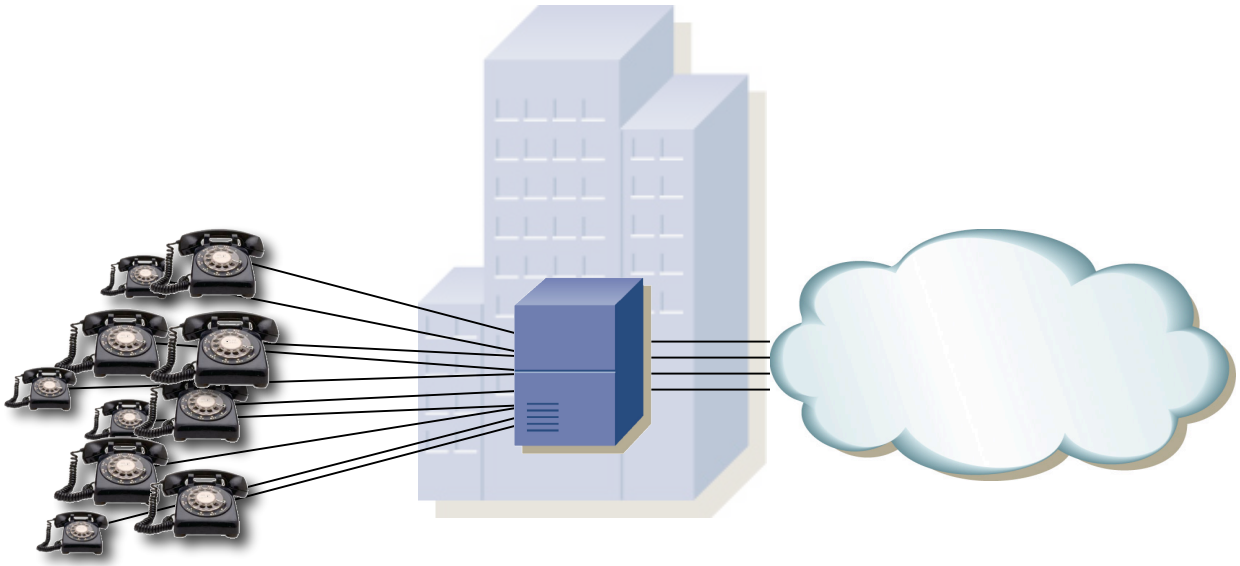
Tiempos de servicio

- Equivalentemente tamaños de paquetes y de ficheros
- ¿Deterministas?
  - Celdas ATM ok
  - ¿Ficheros servidor web?
  - ¿Paquetes IP?
- ¿Exponenciales?
  - Es una distribución continua. ¿Aproximado?
  - ¿Los ficheros que piden los usuario tienen esa distribución?
  - ¿Los tamaños de los paquetes IP?
- ¿Independientes?

M/M/c/c

Servicio telefónico (Erlang)

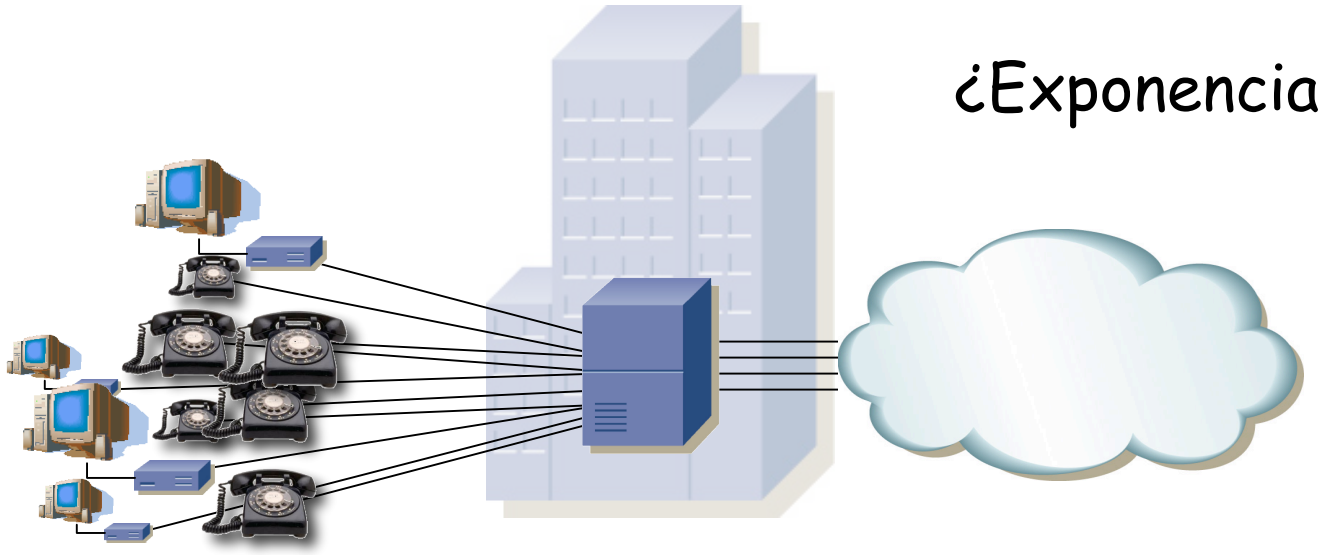
- Gran número de usuarios
- Tiempo entre llamadas a una central: exponenciales independientes
- Duración de las llamadas: exponencial
- c líneas externas
- Nos permite calcular la probabilidad de que una llamada encuentre una línea libre
- Estupendo, pero un buen día…



M/M/c/c

Servicio telefónico

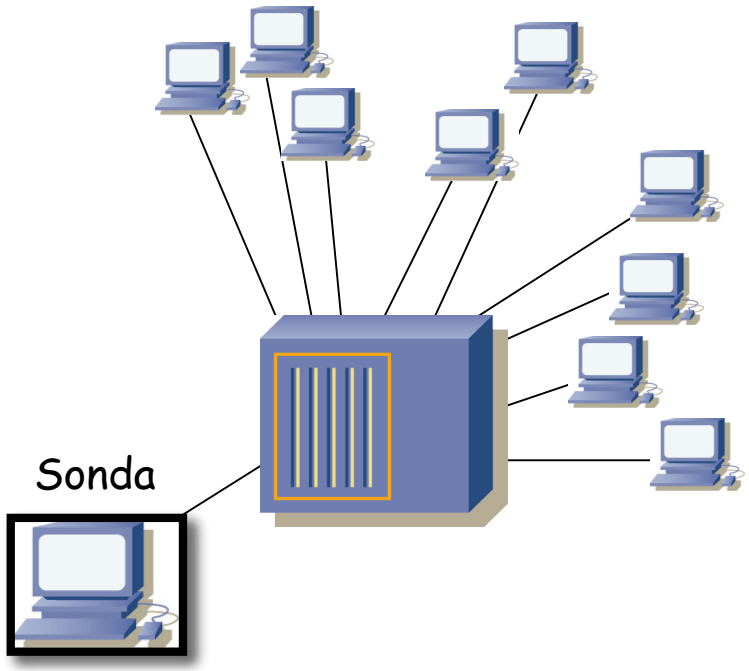
- Gran número de usuarios
- Tiempo entre llamadas a una central: exponenciales independientes
- Duración de las llamadas: exponencial
- c líneas externas
- Nos permite calcular la probabilidad de que una llamada encuentre una línea libre
- Estupendo, pero un buen día…



Captura de tráfico

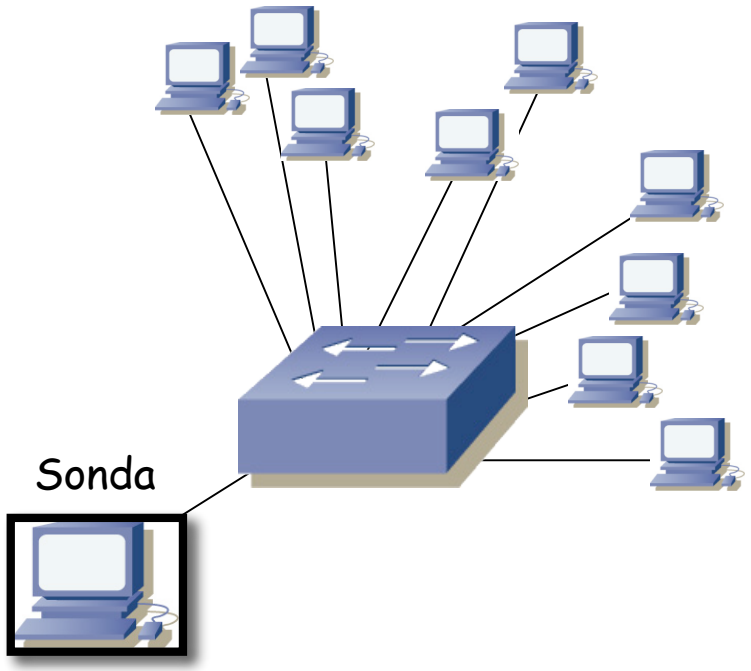
¿Cómo se captura el tráfico?

- Hub y *sniffer* (tcpdump, programa ad-hoc, etc)
- Trazas a disco
- Análisis en tiempo real



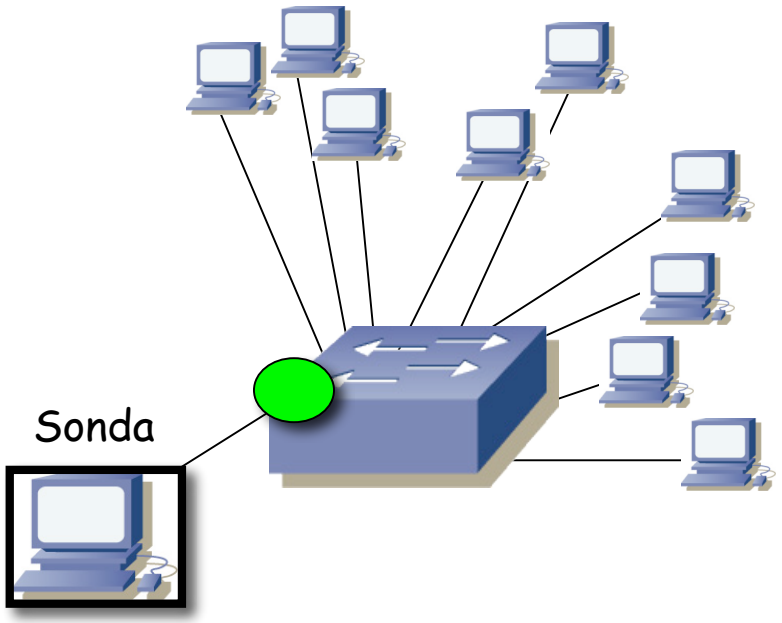
¿Cómo se captura el tráfico?

- Switch con *SPAN* y *sniffer*
- Trazas a disco
- Análisis en tiempo real



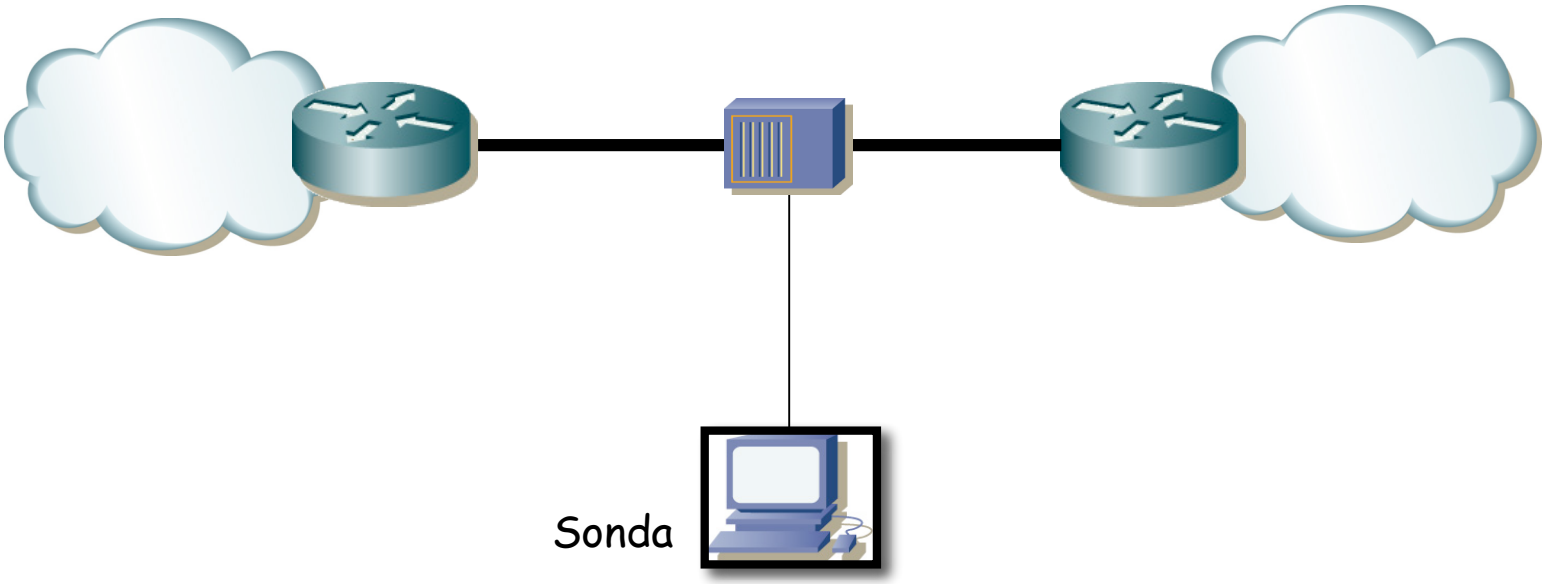
¿Cómo se captura el tráfico?

- El conmutador puede recoger estadísticas
- Normalmente resumidas
- La sonda recogería periódicamente esos resúmenes
- También aplica a routers
- Ejemplo: NetFlow



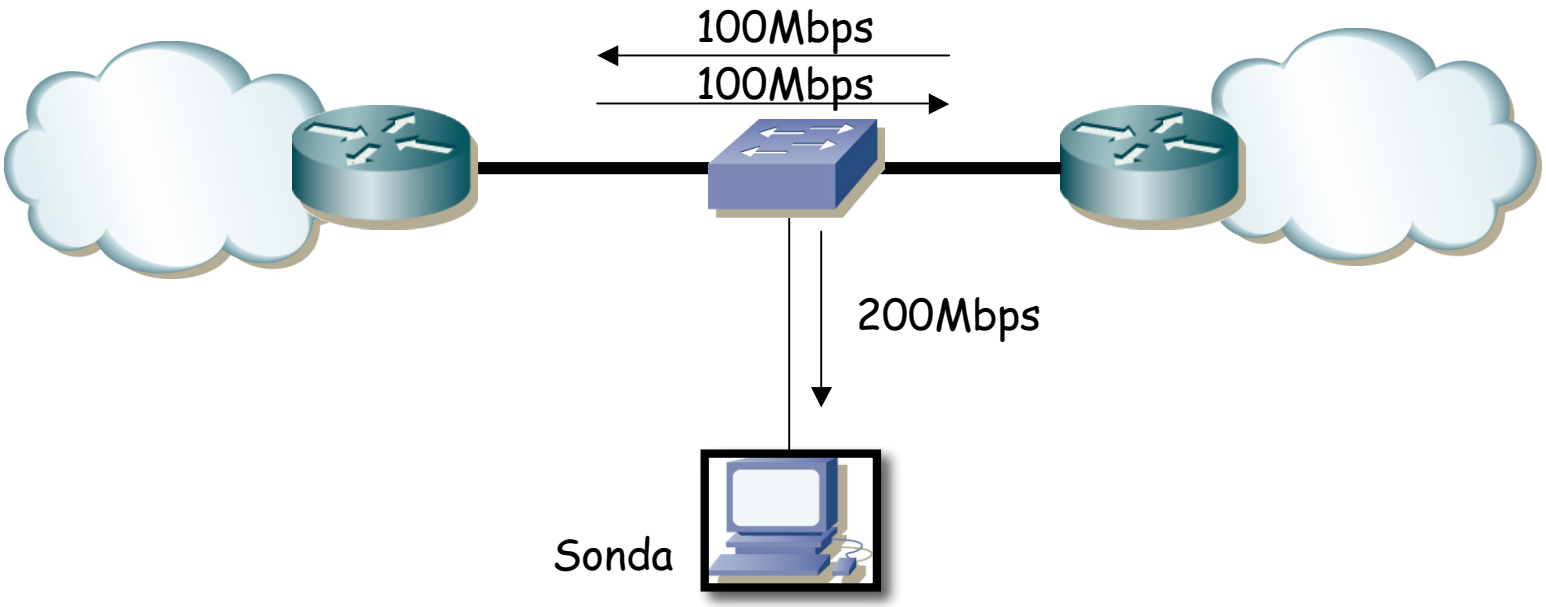
¿Cómo se captura el tráfico?

- Enlace entre 2 routers (…)
- Poner un hub
  - Solo para 10/100 Ethernet
  - Podría para Gigabit pero no se fabrican hubs
  - Se pierde el full duplex, puede haber colisiones



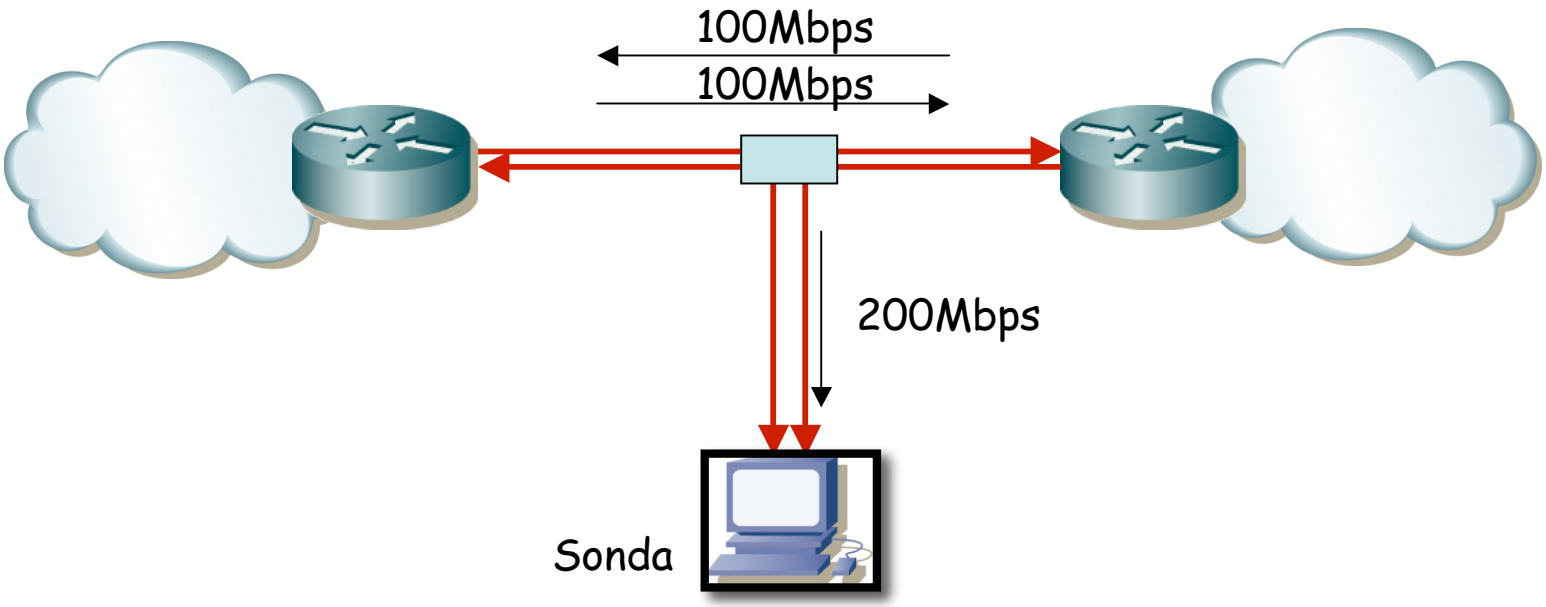
¿Cómo se captura el tráfico?

- Enlace entre 2 routers
- Poner un switch con *SPAN*
  - Con full duplex el tráfico a monitorizar es 2x la velocidad



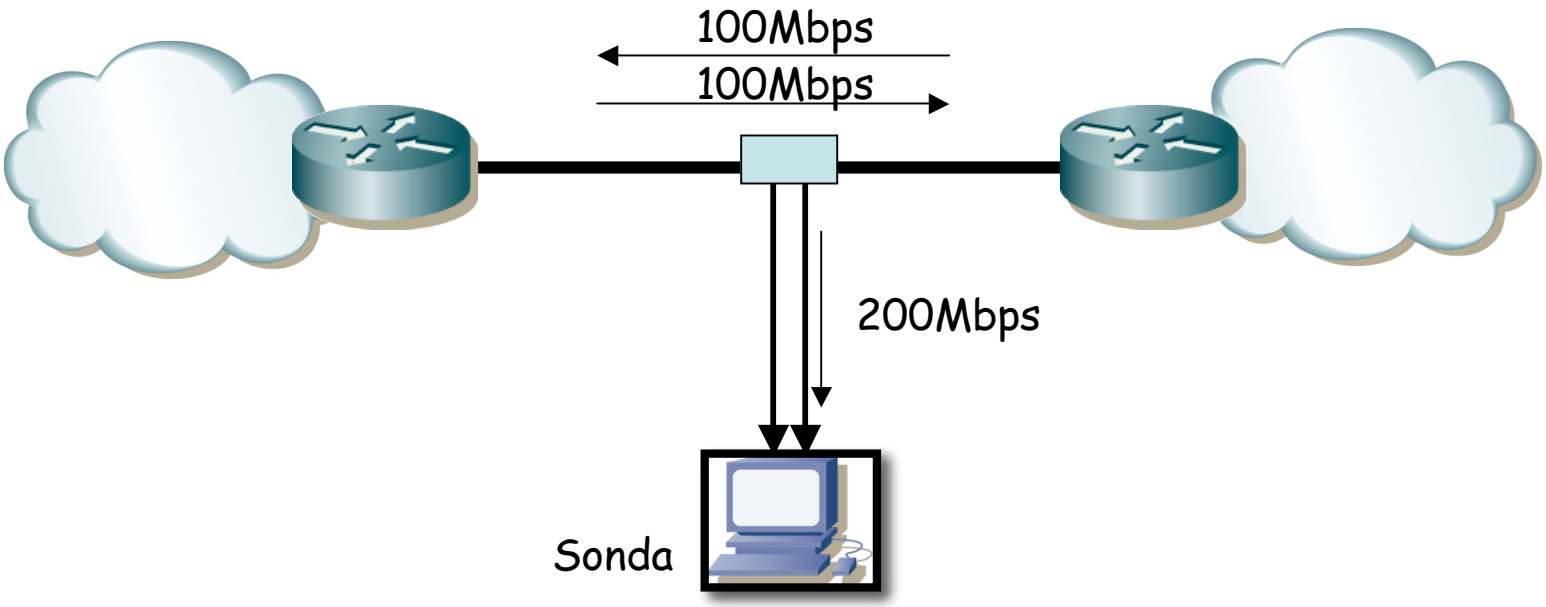
¿Cómo se captura el tráfico?

- Enlace **óptico** entre 2 routers
- Poner un splitter
  - Con full duplex el tráfico a monitorizar es 2x la velocidad
  - Normalmente requiere 2 interfaces de red en la sonda (solo RX)
  - Pasivo (resistente a fallos de alimentación)



¿Cómo se captura el tráfico?

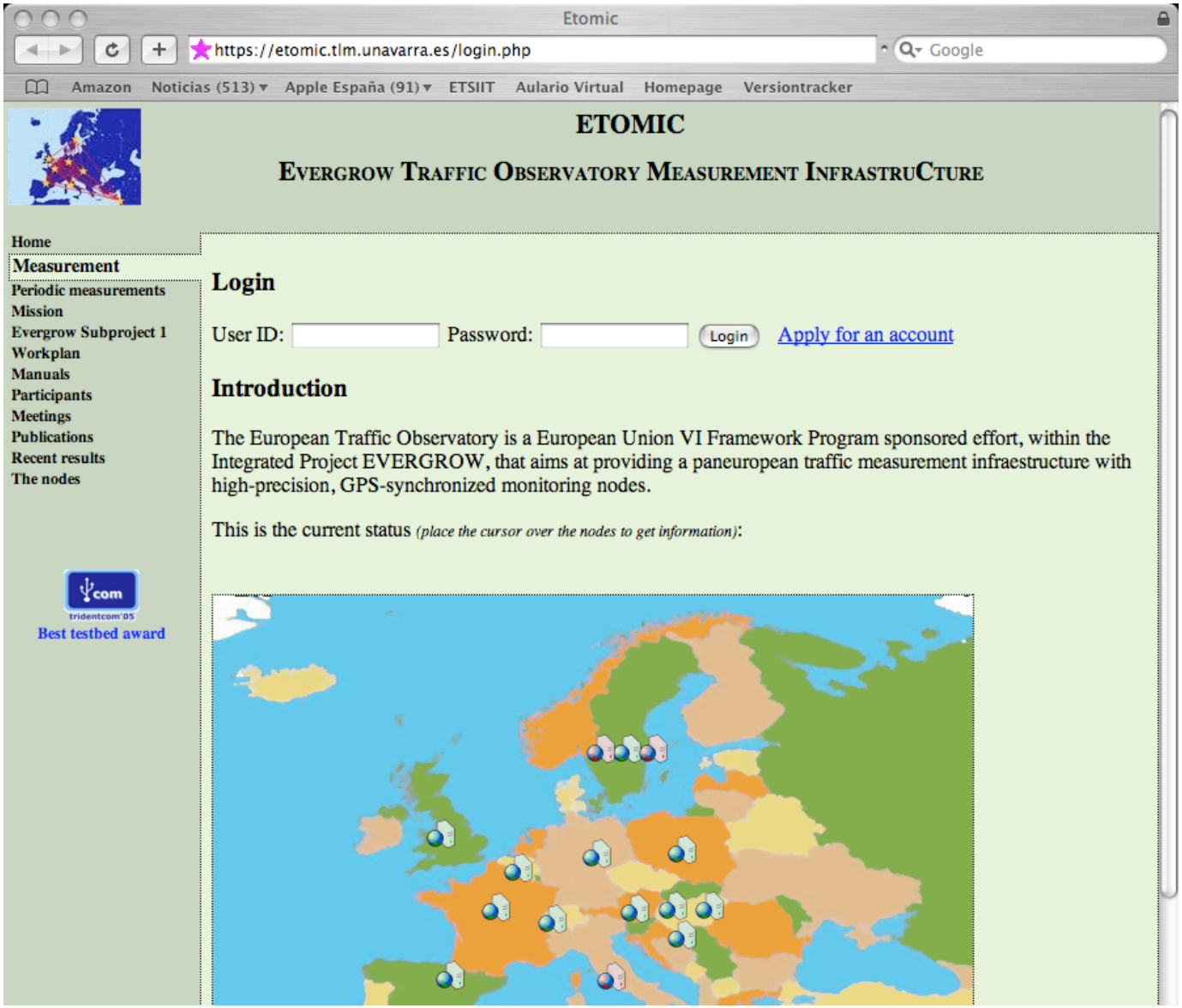
- También existe el splitter (*Tap*) eléctrico
  - Con full duplex el tráfico a monitorizar es 2x la velocidad
  - Normalmente requiere 2 interfaces de red en la sonda (solo RX)
  - Pasivo (resistente a fallos de alimentación)



Medidas activas

- Las sondas generan tráfico
- Hacia servidores u otras sondas
- Recogen información de ese tráfico

ETOMIC


Etomic
https://etomic.tlm.unavarra.es/login.php
Google
Amazon
Noticias (513)
Apple España (91)
ETSIIT
Aulario Virtual
Homepage
Versiontracker
ETOMIC
EVERGROW TRAFFIC OBSERVATORY MEASUREMENT INFRASTRUCTURE
Home
Measurement
Periodic measurements
Mission
Evergrow Subproject 1
Workplan
Manuals
Participants
Meetings
Publications
Recent results
The nodes
Login
User ID:
Password:
Login
Apply for an account
Introduction
The European Traffic Observatory is a European Union VI Framework Program sponsored effort, within the Integrated Project EVERGROW, that aims at providing a paneuropean traffic measurement infraestructure with high-precision, GPS-synchronized monitoring nodes.
This is the current status (place the cursor over the nodes to get information):
tridentcom'05
Best testbed award

Artículos

Papers que vamos a ver

- R. Jain and S.A. Routhier, *"Packet Trains - Measurements and a New Model for Computer Network Traffic"*, IEEE Journal on Selected Areas in Communications, vol. SAC-4, no. 6, Sept. 1986

- C. Fraleigh, S. Moon, B. Lyles, C. Cotton, M. Khan, D. Moll, R. Rockell, T. Seely and C. Diot, *"Packet-Level Traffic Measurements from the Sprint IP Backbone"*, IEEE Network, vol. 17, no. 6, Nov/Dec. 2003

- F. Hernández-Campos, K. Jeffay and F.D. Smith, *"Tracking the Evolution of Web Traffic: 1995-2003"*, Proc. Of the 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems 2003

Objetivos de la presentación

- Explicar lo que has hecho y que se entienda
- Convencer de que
  - El tema es interesante
  - Es importante
  - Has aportado algo
  - Lo has hecho correctamente
- ¡ Pero solo si es así !
- Vender el trabajo (marketing)
- Pero sin engañar (ciencia)

Cómo presentarlos

- Di qué artículo vas a presentar y dónde está publicado
- Quiénes son los autores, de dónde son
- Índice de la presentación
- Introducción: tema general, antecedentes
- Escenario: tema concreto, escenario concreto
- Qué hacen
- Qué resultados obtienen
- Qué conclusiones se extraen
- Qué te ha parecido útil
- Qué te parece inútil, incorrecto o mejorable
- Básico:
  - Entérate tú
  - Consigue que se enteren los demás
- 30 minutos

Traffic Analysis

- Introducción -

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Programa de Tecnologías para la gestión distribuida
de la información