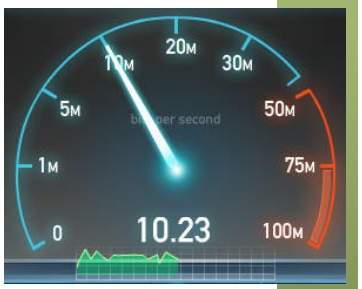
Monitorización de red: Medidas activas

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

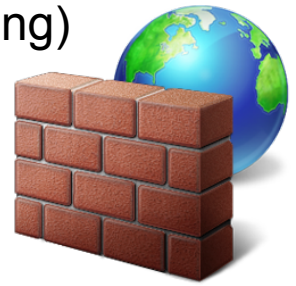
Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

Medidas activas

- ¿Descargarse un fichero grande y medir el throughput medio?
  - Muy intrusivo, pero se hace
  - ¿Cómo de grande? ¿Es significativo el throughput medio?
  - Comprueba throughput a nivel de aplicación (SLA de usuario)
  - No da tanta información a nivel de red



- Mejor que sea menos intrusivo
- Que sea un tráfico pequeño frente al de usuarios
- Que no se vea afectado por mecanismos de seguridad (o sí para evaluarlos)
- Que siga el mismo *data-path* que el tráfico de usuario en los conmutadores (ICMP no siempre lo sigue)
- Que la medida no esté sesgada por ser hecha en un periodo de tiempo corto y afectada por patrones diarios
- Que el tráfico sea “similar” al de los usuarios (tamaños de paquetes, protocolos si se ven afectados en el forwarding)



Medidas activas: ejemplos

Comprobar la disponibilidad de un servidor

- Un *ping* podría valer si nos importa la disponibilidad del host
- Oh, sí, se usa “mucho”
- Desde diferentes *vantage points* pues podría ser accesible desde un punto en la red y no desde otro

Medidas activas: ejemplos

Comprobar la disponibilidad de un servidor/servicio

- Si importa el servicio/aplicación debería ser una comprobación a ese nivel
- Por ejemplo si se puede establecer la conexión TCP con el servidor
- O si se logra descargar un fichero por HTTP
- O si un servidor de DHCP responde ofreciendo una configuración de red
- O comprobar si se puede establecer la señalización SIP con un teléfono
- O hacer una consulta/inserción en una base de datos
- Importante delimitar si la responsabilidad está en la red o en el servicio/servidor pues suelen ser gestionados por distintas personas

Medidas activas: RTT

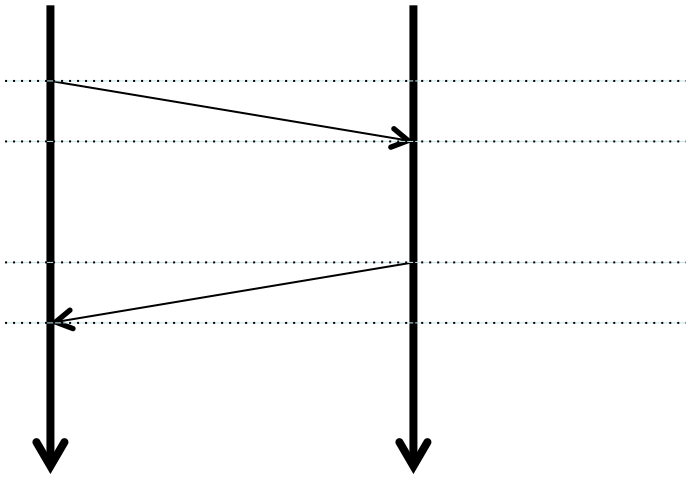
Medidas del retardo

- De nuevo *ping* para RTT
- Cuidado pues el procesado de ICMP puede llevar diferente tiempo
- También un primer paquete puede establecer entradas en caches (enviar varios)

Medidas activas: RTT

Medidas del retardo

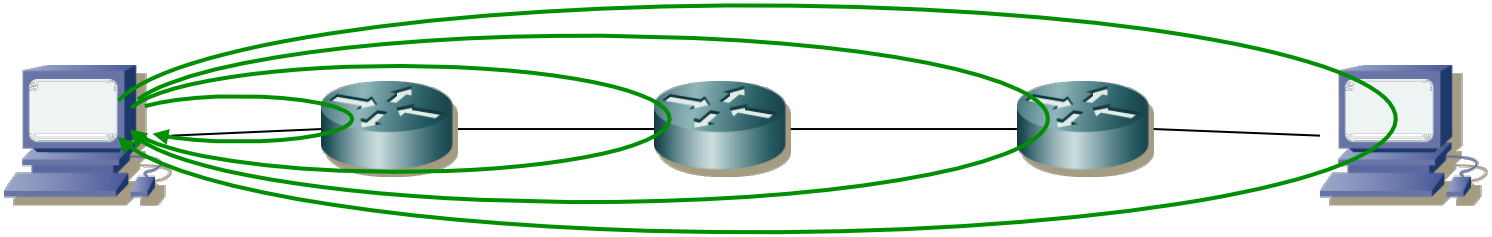
- RFC 5357 “A Two-Way Active Measurement Protocol (TWAMP)”
- Especifica un protocolo para controlar la medida y recoger los resultados (TWAMP-Control, sobre TCP 862)
- Y un protocolo para los mensajes de la medida (TWAMP-Test, sobre UDP)
- Requiere un demonio específico contra el que hacerla
- En la respuesta se incluye el instante en que se recibió el paquete de prueba y en el que se envió la respuesta, para eliminar el tiempo de procesado



Medidas activas: RTT

Medidas del retardo

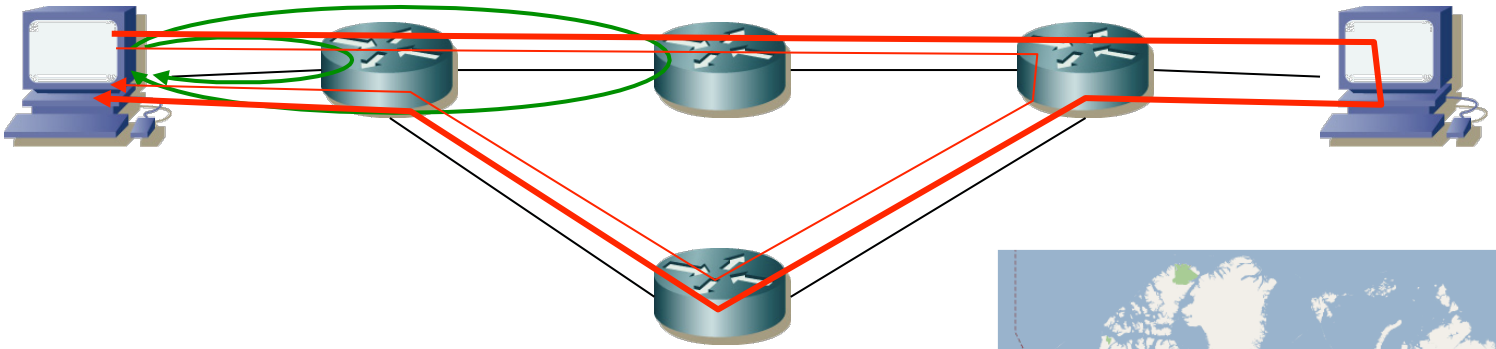
- *Traceroute* permite averiguar el RTT con cada salto del camino
- Además de “descubrir” a esos routers intermedios (solo nivel IP y no todos)
- Asume que el camino es el mismo en ambos sentidos
- (…)



Medidas activas: RTT

Medidas del retardo

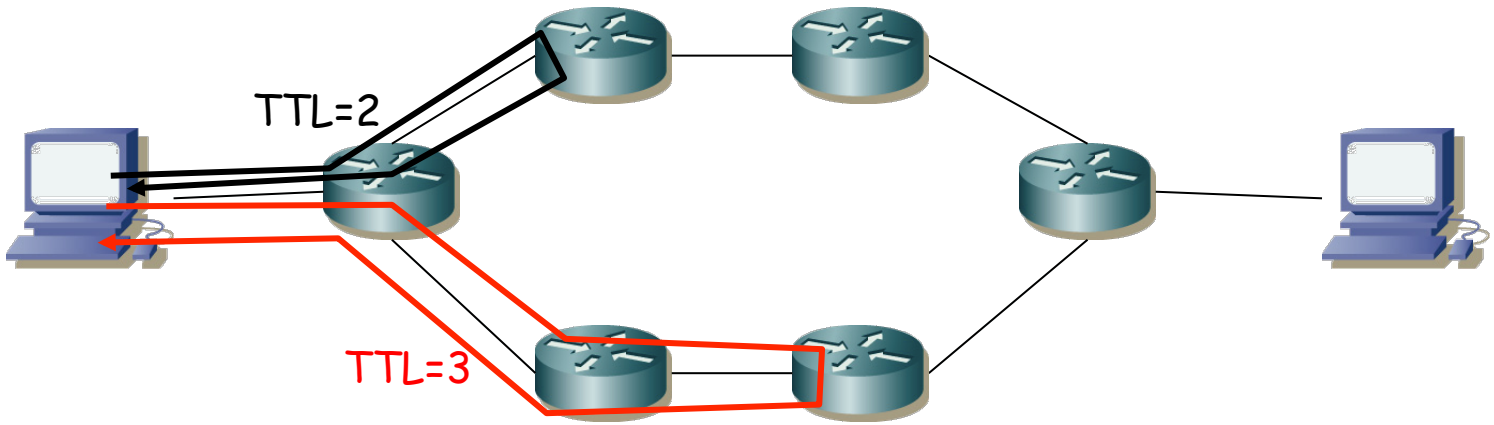
- *Traceroute* permite averiguar el RTT con cada salto del camino
- Además de “descubrir” a esos routers intermedios (solo nivel IP y no todos)
- Asume que el camino es el mismo en ambos sentidos
- Podría no serlo
- (…)



Medidas activas: RTT

Medidas del retardo

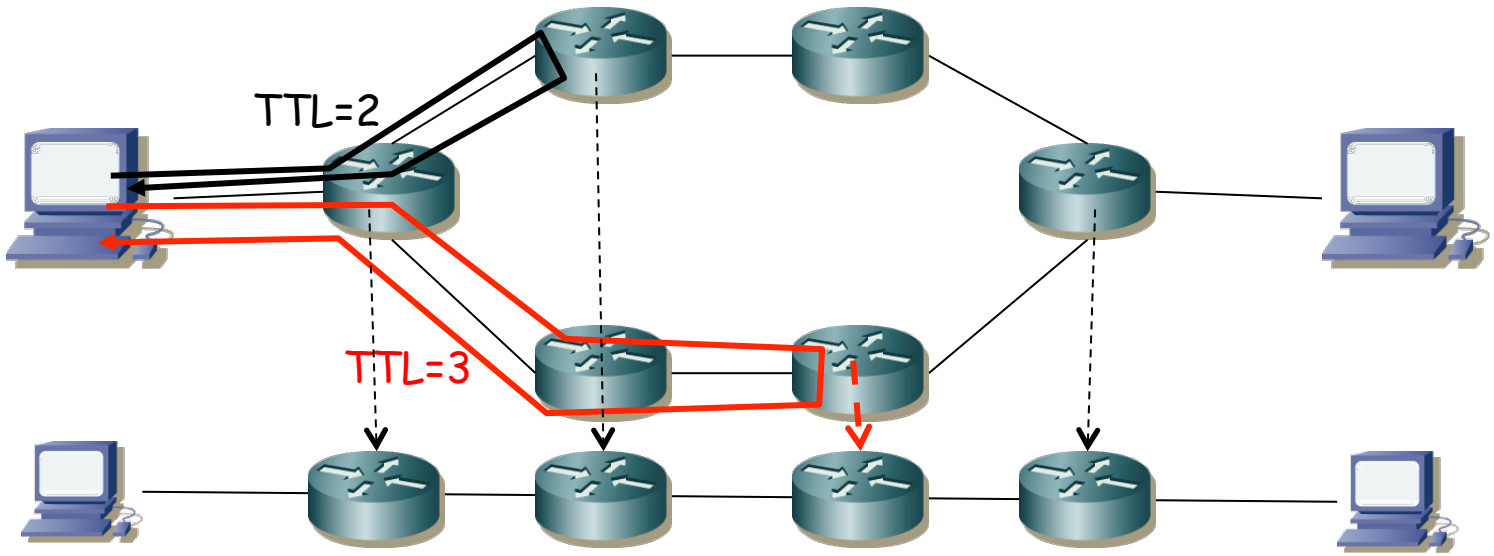
- *Traceroute* permite averiguar el RTT con cada salto del camino
- Además de "descubrir" a esos routers intermedios (solo nivel IP y no todos)
- Asume que el camino es el mismo en ambos sentidos
- Podría no serlo
- Podría haber balanceo de carga por paquete
- Con balanceo por paquete creemos que la red es otra (…)



Medidas activas: RTT

Medidas del retardo

- *Traceroute* permite averiguar el RTT con cada salto del camino
- Además de "descubrir" a esos routers intermedios (solo nivel IP y no todos)
- Asume que el camino es el mismo en ambos sentidos
- Podría no serlo
- Podría haber balanceo de carga por paquete
- Con balanceo por paquete creemos que la red es otra
- Balanceo por paquete también afecta al RTT del *ping* (calculamos uno pero puede que luego la aplicación sufra otro)
- Balanceo por flujo puede hacer que calculemos un path y se use otro



Medidas activas: DISMAN

- Distributed Management Working Group (IETF)
- RFC 4560 “Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations”
- MIB para que un host inicie medidas de ping, traceroute y DNS
- Y para recoger los resultados
- DISMAN-PING-MIB
- DISMAN-TRACEROUTE-MIB
- DISMAN-NSLOOKUP-MIB
- También MIBs propietarias similares

Medidas activas: OWD

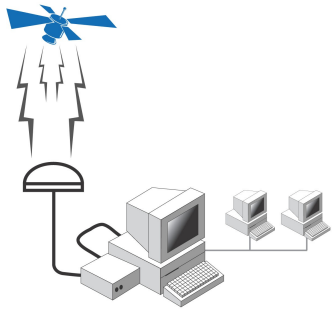
Medidas del retardo en un sentido

- *OWD: One-Way-Delay,* medir el retardo solo en un sentido
- Al medir RTT con caminos asimétricos se mezcla el rendimiento de ambos
- Aunque el camino sea simétrico puede haber diferente cantidad de encolado
- Normalmente lo queremos medir independientemente en los dos sentidos
- Principalmente afecta aplicaciones en tiempo real
- (...)

Medidas activas: OWD

Medidas del retardo en un sentido

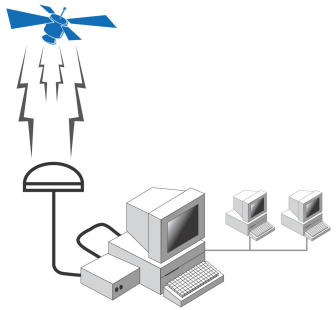
- Requiere cooperación de los dos extremos (no de solo uno como en RTT)
- Requiere sincronización de relojes (NTP o GPS)
- Activa: enviando el paquete
- Pasiva: monitorizando y reconociendo el paquete en las dos sondas
- El valor mínimo da una indicación de retardo con enlaces descargados
- Valores por encima del mínimo da una indicación de congestión en el camino
- RFC 2679 “A One-way Delay Metric for IPPM”
- ITU-T Y.1540 “Internet protocol data communication service – IP packet transfer and availability performance parameters” (IP packet transfer delay, IPTD)



Medidas activas: OWD

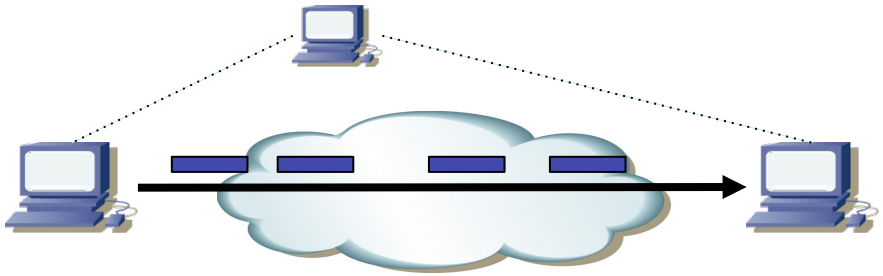
Medidas del retardo en un sentido

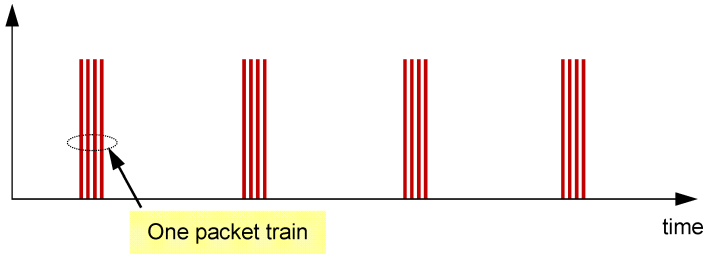
- RFC 4656 “A One-way Active Measurement Protocol (OWAMP)”
- Especifica un protocolo para controlar la medida y recoger los resultados (OWAMP-Control, sobre TCP 861)
- Y un protocolo para los mensajes de la medida (OWAMP-Test, sobre UDP)
- Requiere un demonio específico contra el que hacerla
- http://www.internet2.edu/performance/owamp/
- *owping*



Medidas activas: BW

- *Bulk Transfer Capacity:*
  - Mediante herramientas de transferencia masiva (iperf, nuttcp, thrulay)
  - Soluciones como BWCTL permiten desde un tercer host controlar medidas entre otros dos
- Mediante trenes de paquetes
  - Pueden estimar la capacidad máxima del cuello de botella
  - O el ancho de banda disponible
  - Requieren buena sincronización para medir altas capacidades

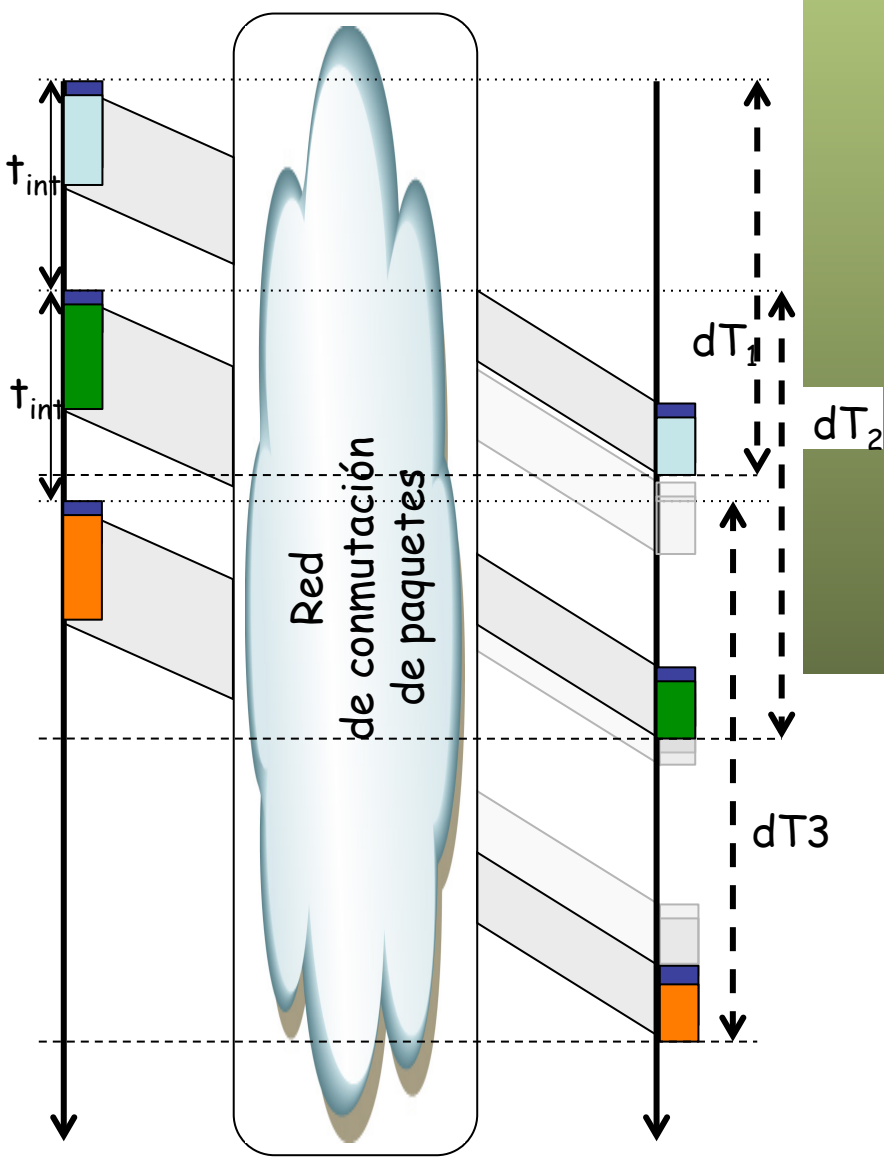




Medidas activas: PDV

Jitter* o *Packet Delay Variation

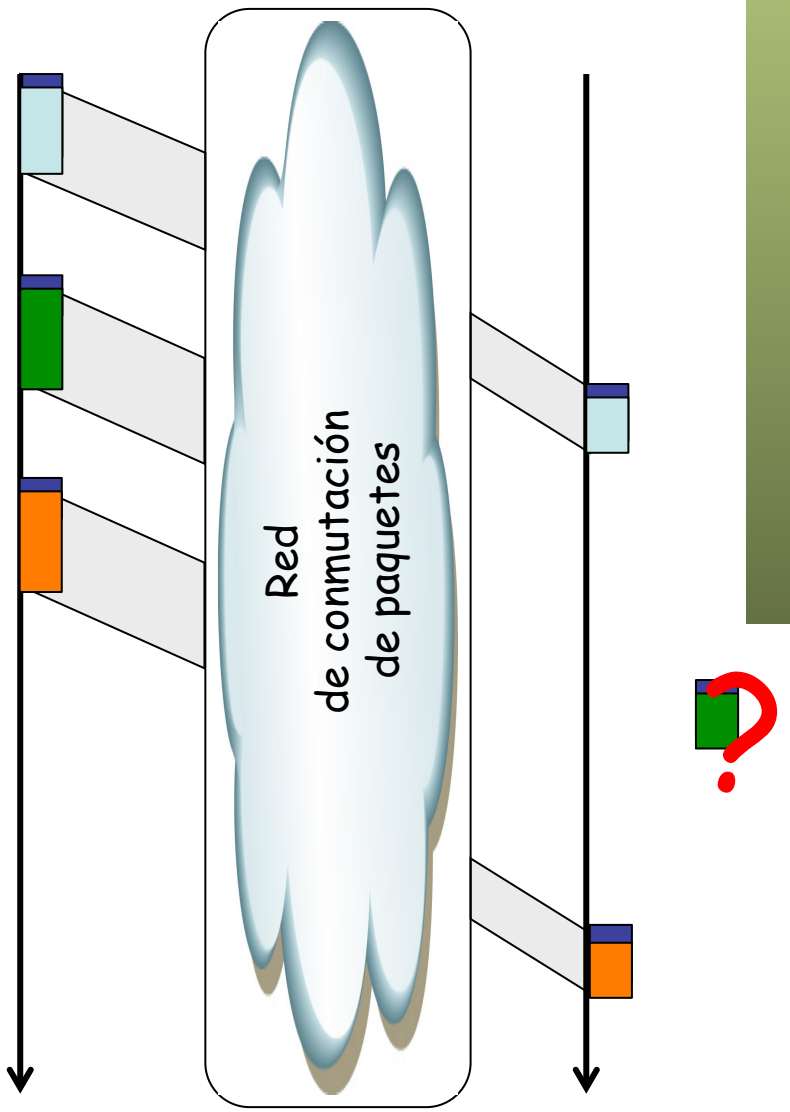
- RFC 3393 "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)"
- Diferentes definiciones (ver discusión en RFC 5481)
- *De-jitter buffer*



Medidas activas: *Losses*

Pérdidas

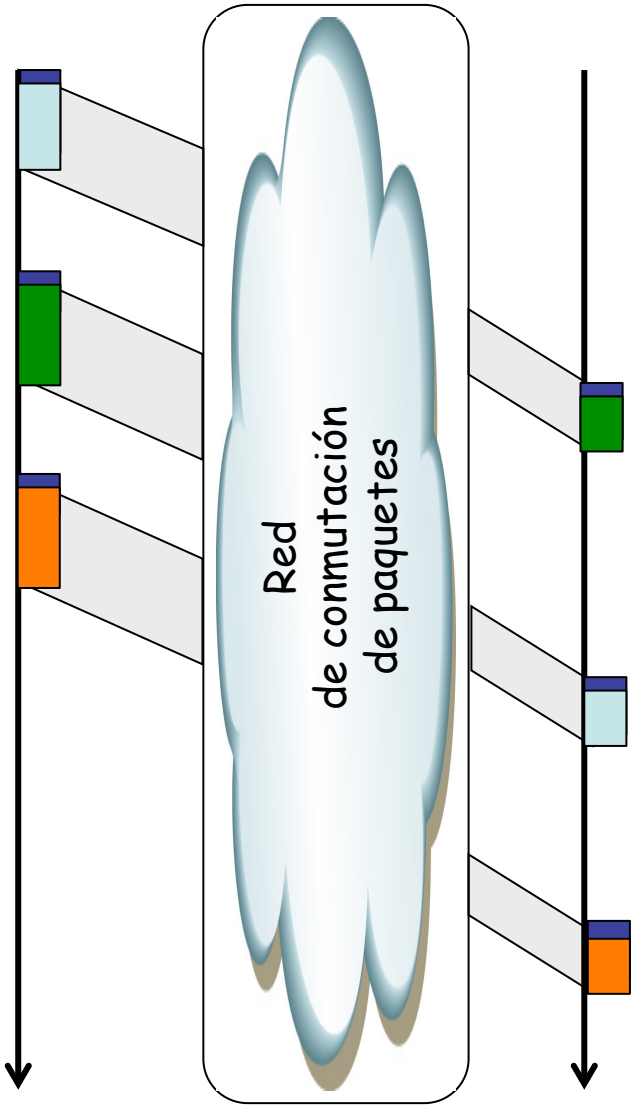
- RFC 2680 “A One-way Packet Loss Metric for IPPM”
- Y.1540 habla de IPLR (IP packet loss ratio)



Medidas activas: *Reorder*

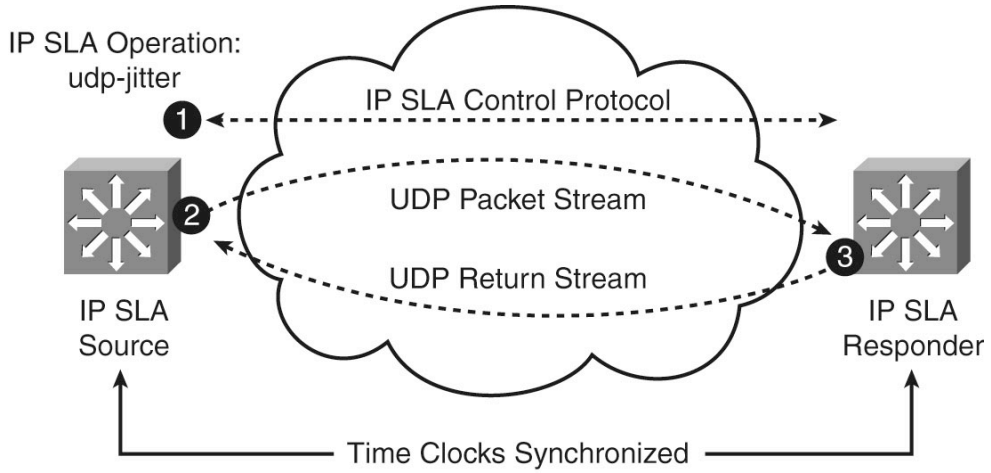
Desórdenes

- RFC 4737 "Packet Reordering Metrics"
- Y.1540 habla de IPRR (IP packet reordered ratio)



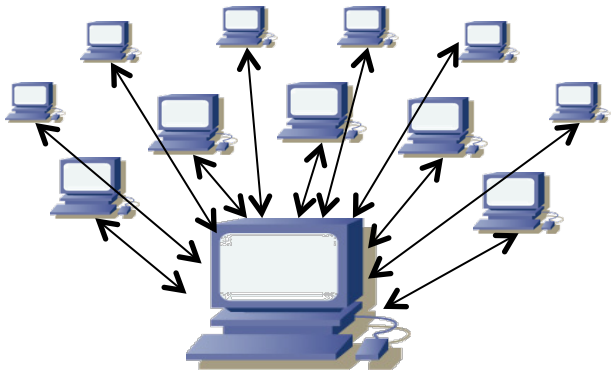
Ejemplo: Cisco SLA

- Un equipo actúa como *Sender* y otro como *Responder*
- Una primera fase de control que inicia el *sender*
- Mensajes en la fase de control UDP puerto 1167
- Especifican las medidas a hacer, a qué puerto
- A continuación fase de medida
  - De red: delay (OWD y RTT, TWAMP), jitter y pérdidas
  - De aplicación: DNS, DHCP, TCP connect, HTTP, VoIP UDP Jitter, VoIP Post-Dial Delay, FTP (download file), HTTP (DNS+connect+download)
  - De enlace: específicas de Frame Relay, ATM
- RFC 6812 (Informational) "Cisco Service-Level Assurance Protocol" mensajes del protocolo, no cómo hacer las medidas



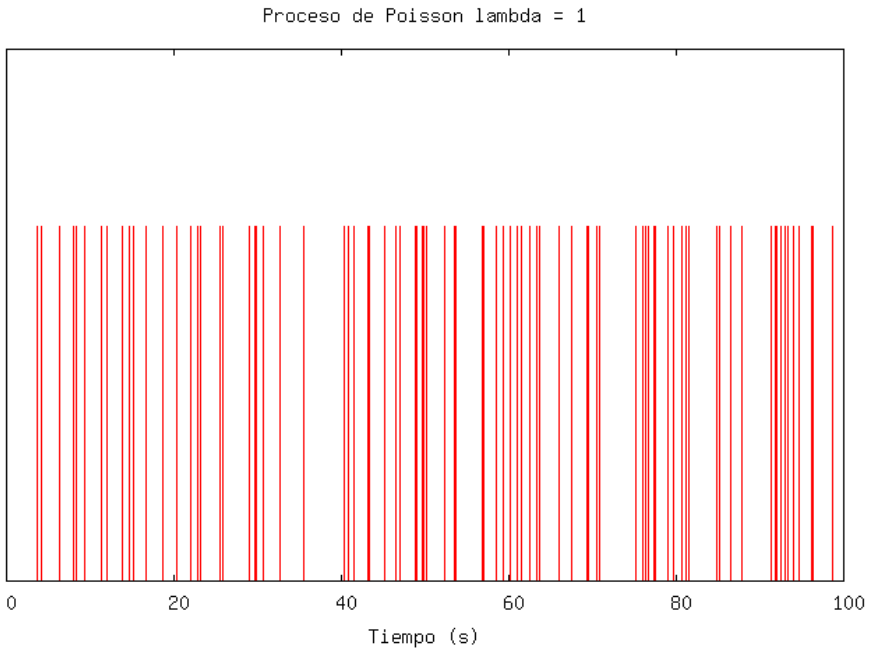
¿Cuándo hacer las medidas?

- Medidas desde un host a varios destinos
  - Cuidado si gran cantidad de destinos son sondeados simultáneamente
  - Se interfieren las medidas
  - Pueden suponer una carga apreciable para el host
  - O para los enlaces
- Medidas desde un host, una al terminar la anterior
- Periodo de repetición del bloque
- O repetición tras un tiempo aleatorio



¿Cada cuánto medir?

- Medidas a un host
- Periódicas pueden perder eventos también periódicos
- En general resultados sesgados
- Mejor medidas en instantes “aleatorios”
- Lo “más aleatorio” son tiempos exponenciales
- Es decir, un proceso de Poisson para los instantes de medida



Activas vs Pasivas

- Activas toman medidas haciéndose pasar por tráfico de usuario
- Activas sirven para medir ciertos parámetros de SLA
- Activas pueden medir en el camino *end-to-end*
- Y pueden hacer inferencias de otros parámetros
- Activas pueden detectar el problema pero no la causa
- No sirven para medir tráfico por protocolo, usuario, etc (para eso pasivas)
- Pasivas permiten identificación de aplicaciones en el tráfico
- Estadísticas de uso de protocolos, hosts y servicios
- Permiten calcular utilización
- Pero no te dicen directamente lo que experimenta el tráfico de usuario (retardos, pérdidas)