

Control 1

Redes

Plazo de entrega: 11 de septiembre de 2024

José M. Piquer

Intro

El control se responde en forma individual, sin preguntas entre Uds o a terceros. Todas las dudas pregúntenlas en el foro de U-cursos y el equipo docente les responderá. Entreguen las tres preguntas en un PDF con su nombre por U-cursos. Pueden (y deben) buscar material en Internet para responder, pero citen siempre las fuentes que utilizan. Pueden usar chatGPT para ayudarlos, pero, no pueden entregar su respuesta directamente, deben explicar y analizar todo lo que les propone. Recuerden que chatGPT se equivoca, alucina y miente con mucha convicción. Siempre recuerden mencionarlo si lo utilizan.

En épocas de chatGPT estamos obligados a evaluar mal respuestas que antes habríamos aceptado como casi correctas. Si Uds entregan un párrafo de argumentos correctos pero no responden nunca la pregunta específica con argumentos técnicos que corresponden a ese caso, hoy en día tienen cero puntos.

Un ejemplo, decir algo como: “existen algoritmos propuestos con mejoras para TCP para enlaces de alto delay como CUBIC y BBR, que buscan resolver este problema” antes les habrían dado algún puntaje (significaba que habían hecho una búsqueda en google al menos). Hoy en día vale cero.

Las preguntas de los controles las chequeamos con chatGPT antes de ponerlas, y la idea es que chatGPT no logre sacarse un 4.0.

Entonces, la recomendación es: contesten la pregunta específica del enunciado. Las frases periféricas que buscan adornar sin ir al detalle técnico no aportan en nada, de hecho más bien perjudican, por que mientras más hablan sin ir al punto, más generan la impresión en el corrector que no conocen la respuesta (y suenan igual que chatGPT).

P1: sockets

Para la Tarea 1, probamos con tres servidores de echo distintos: con procesos pesados, con threads y con select. Si a Ud lo contratan para usar esta solución para hacer un verdadero medidor de ancho de banda para una red corporativa de una empresa grande con sucursales en todo el país, responda las siguientes preguntas:

1. ¿cómo elegiría el servidor a usar?
2. Para cada servidor, trate de construir un escenario donde ese sea el mejor candidato para resolver el problema.
3. Diseñe una configuración que permita medir ancho de banda permanentemente dentro de la red, de modo de permitir detectar fallas y congestión automáticamente: ¿dónde pondría los servidores? ¿desde dónde correrían los clientes?
4. Alguien propone que cambien el socket TCP por uno UDP para que sea más eficiente la medición. ¿es buena idea? ¿por qué?
5. El servidor podría estar ejecutando muchas veces en paralelo y entonces: ¿puede afectar el resultado de las mediciones? ¿Tendría el servidor que limitar el número de clientes que atiende?
6. Modifique los servers 2, 4 y 5 para que atiendan un máximo de MAX-PROCS clientes a la vez. Entregue acá el código modificado.

P2: DNS

2.1 Algoritmo Resolver

Un resolver debe elegir siempre a quién realmente preguntar de la lista de NS para un dominio dado. Una propuesta muy utilizada es ir anotando el tiempo de respuesta de cada NS y luego privilegiar los más rápidos (son los más cercanos y los menos cargados). El problema es que, para aprender cómo van cambiando las cosas en el tiempo, debemos enviar algunas preguntas a los más lentos también. Incluso a los que no responden, ya que podrían estar respondiendo ahora.

1. Escriba un pseudo-código del algoritmo que Ud implementaría en un resolver para la función `GetNameServer(ns_list)`, que recibe una lista de servidores y elige el próximo a usar.

2. ¿Sería buena idea preguntarle a todos los NS en paralelo y así garantizar una respuesta rápida siempre? Justifique

2.2 DNS obsoletos respondiendo

Un problema de los servidores DNS es que la gente de olvida de ellos. Entonces, hay servidores DNS gratis en la red que uno los usa y luego los deja de usar pero ellos siguen respondiendo por el dominio. Por ejemplo, Uds pueden haber sido dueños del dominio `dcc.cl` por un tiempo, e inscribieron su nombre en NIC Chile y le configuraron un servidor primario y secundario en CloudDNS.

Ahora ya no lo usan, pero nunca hicieron ningún trámite, por lo que CloudDNS sigue anunciándolo como un dominio válido. Pasada la fecha de renovación, NIC Chile lo borra de su registro, pero CloudDNS sigue anunciándolo.

¿Es esto grave? ¿Afecta a los que le consultan por dominios a CloudDNS? ¿Puede ser eventualmente peligroso?

2.3 Contienda de Competencia

La lista de servidores de un dominio está en dos partes distintas: en el padre que dice que ese dominio existe y quiénes son sus servidores, y en la zona misma del dominio que se configura en el servidor primario. Esto es fuente de muchos errores, ya que la zona padre está en un servidor y la zona del primario está en otro, por lo que fácilmente divergen.

1. Explique por qué esto tiene que ser así, a pesar de los problemas que conlleva.
2. Si las listas son distintas, ¿cuál manda?
3. Si las dos listas no contienen ningún servidor en común, ¿qué pasará?

P3: Proxy https

Vimos en la actividad evaluada 2 que cada vez hay menos servidores http puros y todos están migrando a https. El principal cambio es que ahora se usa un "Transport Layer Security (TLS)", que es como un socket encriptado que además exige un certificado de validación al servidor. Esto no parece demasiado cambio al protocolo, y sería interesante poder hacer un proxy-copy

https como el de la actividad evaluada 2, que registre todos los comandos y respuestas en un archivo.

En Internet, hay dos posibles soluciones de proxies https que son bastante populares:

1. CONNECT: es un comando HTTP que sólo interpretan los proxies y les permiten establecer conexiones HTTPS. El proxy normal interpreta él este comando en vez de simplemente pasarlo al servidor.
2. <https://mitmproxy.org/> es un proxy que permite al browser conectarse con él en forma “segura” y luego al verdadero servidor usando HTTPS.

Compare ambas soluciones y analice si servirían para la actividad 2 del curso, pero ahora soportando sitios https. No es necesario ir a mirar el código o hacer pruebas reales. Pero sí lean la documentación de cómo funcionan y explique sus argumentos.

Lecturas recomendadas:

1. <https://www.internetsociety.org/deploy360/tls/>
2. https://en.wikipedia.org/wiki/HTTP_tunnel