Solución Examen – 24 de febrero de 2010
(ref: sirc1003.odt)

Instrucciones

•Indique su nombre completo y número de cédula en cada hoja.
•Numere todas las hojas e indique la cantidad total de hojas que entrega en la primera.
•Escriba las hojas de un solo lado.
•Utilice una caligrafía claramente legible.
•Comience cada pregunta teórica y cada ejercicio en una hoja nueva.
•Sólo se contestarán dudas de letra. No se aceptarán dudas de ningún tipo los últimos 30 minutos del examen.
•El examen es individual y sin material.
•Es obligatorio responder correctamente al menos 15 puntos en las preguntas teóricas.
•El puntaje mínimo de aprobación es de 60 puntos.
•Para todos los ejercicios, si es necesario, puede suponer que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).
•Duración: 3 horas. Culminadas las 3 horas el alumno no podrá interactuar de ninguna forma con las hojas a entregar, salvo leerlas.

Preguntas Teóricas

Pregunta 1 (8 puntos)

a) Dados dos hosts A y B, con sus respectivas direcciones IP y MAC notadas como sigue IP_A, IP_B, MAC_A y MAC_B. Describa los mensajes ARP intercambiados entre A y B que permiten a A determinar la dirección MAC de B. Deberá indicar al menos direcciones MAC e IP utilizadas en cada mensaje, tanto a nivel de los cabezales Ethernet y payload ARP.
b) Compare el protocolo Neighbor Discovery de IPv6 con el ARP en términos de funcionalidad, capas a las que les provee/consume servicios y sus tipos de mensajes.

a) A-> B ARP Request con:
Src MAC: MAC_A
Dst MAC: ff:ff:ff:ff:ff:ff
Payload

Sender MAC Addr	*MAC_A*
Sender IP Addr	*IP_A*
Target MAC Addr	*00:00:00:00:00:00*
Target IP Addr	*IP_B*

B-> A ARP Reply con:
Src MAC MAC_B
Dst MAC MAC_A
Payload

Sender MAC Addr	*MAC_B*
Sender IP Addr	*IP_B*
Target MAC Addr	*MAC_A*
Target IP Addr	*IP_A*

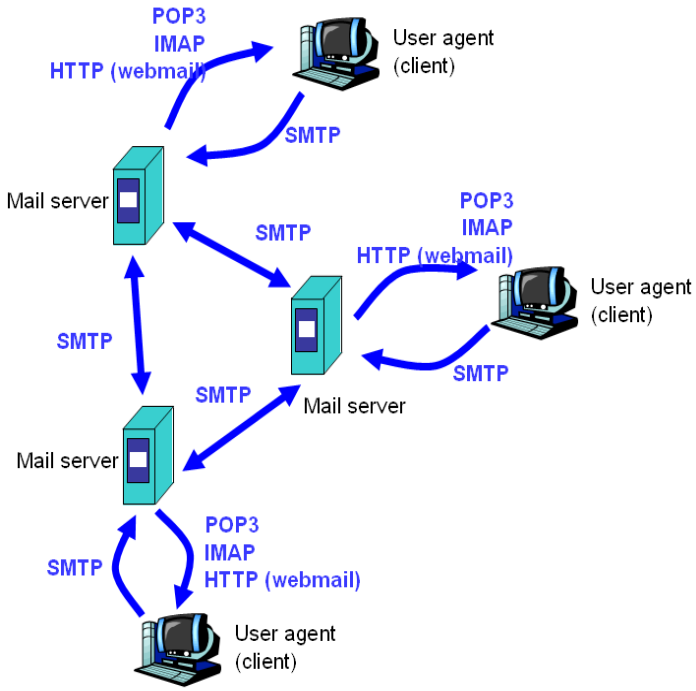
b) ARP es un protocolo definido a nivel de Ethernet (0x0806) "independiente" de IP (0x0800). Es un protocolo auxiliar de la suite TCP/IP. En IPv6, el protocolo ND está definido dentro de ICMPv6 y utiliza ICMPv6, sobre IPv6. De esta forma, la resolución de direcciones de enlace queda resuelta dentro de la propia suite de protocolos y por ello "IPv6 es una implementación más limpia que IPv4".

Pregunta 2 (8 puntos)

a)Dibuje un diagrama que describa la arquitectura de la aplicación correo electrónico. En el diagrama debe indicar cuáles son los roles de los sistemas que participan y los protocolos de aplicación que conozca que se pueden utilizar para intercambiar información entre ellos.

b)Describa la serie de pasos que se aplican sobre un correo electrónico desde que el emisor lo escribe hasta que el destinatario lo lee, asumiendo que el emisor y el destinatario tienen casillas de correo de servidores distintos.

Solución parte a)



Solución parte b)
•El emisor escribe el mensaje de correo electrónico.
•El user agent del emisor envía por SMTP el correo a su mail server.
•El mail server del emisor envía por SMTP el correo al mail server del destinatario.
•El mail server del destinatario almacena el correo en la casilla.
•Más tarde, el destinatario se conecta a su mail server. Si utiliza POP3 o IMAP descarga el correo a su máquina. Si utiliza un webmail lo puede leer en el browser (descarga el correo por HTTP).

Pregunta 3 (8 puntos)

a)¿Qué es el protocolo PPP? ¿Qué es lo que lo hace más simple que otros protocolos que se ejecutan en la misma capa como por ejemplo CSMA?

PPP (point-to-point protocol) es un protocolo de capa de enlace que se utiliza para enviar y recibir datos entre dos entidades en un enlace punto a punto.
Es más simple que los protocolos de acceso al medio de la capa de enlace debido a que no se utiliza en un medio broadcast, donde muchos emisores necesitan competir a la vez por el canal, por lo tanto no se necesita un direccionamiento MAC explícito.

b)PPP utiliza flags para delimitar sus mensajes. Indique cómo es el mecanismo por el cual se logra distinguir entre el contenido de los mensajes y las flags que lo delimitan.

PPP delimita las tramas utilizando un byte especial considerado como <flag> al inicio y al fin de cada trama. Si este byte aparece en algún punto del contenido del mensaje se realiza byte stuffing del mismo utilizando un byte de <escape>:
•El emisor agrega un byte <escape> antes de cualquier byte <flag> o byte <escape> que esté en el contenido que debe enviar.

•Si el receptor encuentra un byte <flag>, considera que es el inicio o el fin de una trama. Si encuentra un byte <escape>, lo descarta y considera el siguiente byte como parte del contenido de la trama.

Pregunta 4 (8 puntos)

En el contexto de la gestión de las redes de computadoras,

a)Explique los conceptos “agente” y “gestor”.

Agente: Entidad (generalmente de software) residente en un sistema gestionado que se encarga de colectar información de gestión. Puede generar notificaciones (traps, alarmas). Generalmente implementado en sistemas de escasos recursos (procesador, memoria). Puede colectar información, pero no toma decisiones en base a ellas (excepción: RMON).
Gestor: Entidad que se encarga de recoger la información de gestión de los diferentes agentes. Interfaz de usuario. Inteligencia de la gestión. Un gestor por muchos agentes. Interoperación entre gestores: Gestión integrada y distribuida.

b)Describa brevemente el modelo de información MIB (*Management Information Base*).

Modelo de Información: Agente y gestor pueden ser de diferentes proveedores y/o versiones… Se necesita un modelo de información de gestión estandarizado; una opción: MIB.
En el contexto del modelo MIB Todo recurso de red gestionable debe ser representado a través de un objeto. Un objeto (en este contexto) es una variable que contiene la información del recurso (diferentes tipos según el recurso, etc). El conjunto de todas las variables conocidas por un agente es la MIB de este agente. El gestor implementa su funcionalidad accediento a los objetos presentes en la MIB de cada agente a gestionar. Lo que se puede hacer con cada agente depende de la MIB implementada por este

Pregunta 5 (8 puntos)

Considere flujos TCP que atraviesan redes inalámbricas y móviles sustentadas en tecnologías como las vistas en clase; mencione y describa brevemente:

a)el principal problema que pueden encontrar dichos flujos y las aplicaciones que se sustentan en ellos para intercambiar información.

TCP interpreta pérdida como señal de congestión, por lo tanto decrementa, a veces innecesariamente, la ventana de congestión.

b)las posibles soluciones y/o paliativos a lo expresado en la parte anterior.

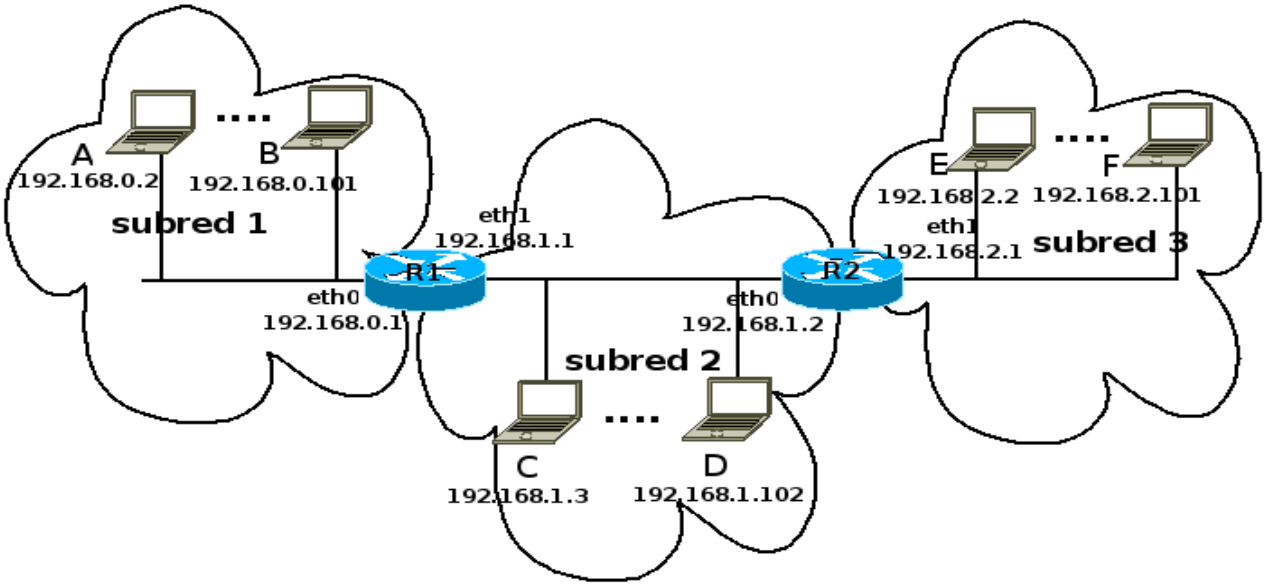
Dos “familias de soluciones” posibles (por lo menos las más difundidas en los ambientes académicos y de la industria):
1- Split de la conexión: TCP para wireless y TCP para wired.
2- Distinguir entre pérdidas por hostilidad del medio y pérdidas por congestión.
La familia 2 es la que ha logrado mayores “adeptos”. Si bien muchos SOs la soportan, por defecto no se encuentra habilitado.La idea básica es que cuando algún router que por el que pasa determinado flujo TCP detecta una congestión incipiente en parte del camino entre emisor y receptor, inicia un marcado de los paquetes informando de ello. De esta forma las entidades TCP son informadas de la situación y considerando la premisa de que la congestión no aparece y desaparece de forma repentina, si un segmento perdido está “rodeado” en lo que respecta a su número de secuencia de segmentos “marcados” se puede deducir que se perdió por efectos de congestión de la red; en caso contrario, se puede concluir que la pérdida se debió a hostilidad del medio por donde atravesó el paquete que lo transportaba.
La implementación estandarizada es ECN (Explicit Congestion Notification).

Información adicional: RFC 3168, 3540, 4774. Señalizar utilizando 2 bits en el encabezado IP y 2 en el TCP, que efectivamente se está experimentando congestión. Soportado en MAC OS, Windows Vista, Linux, Cisco, Solaris 9, tcpdump, wireshark, ns-2,... http://www.icir.org/floyd/ecn.html

Problemas Prácticos

Problema 1 (30 puntos)

Sea la red compuesta por tres subredes interconectadas por los routers R1 y R2 presentada en la siguiente figura.



En la misma se indican los nodos conectados en cada subred así como la dirección IP de cada interfaz. Para su direccionamiento se asignó una red /24 a cada una de las subredes como se presenta en la figura, y se supone la existencia de 100 hosts en cada subred . El enrutamiento es estático.

Se pide:

a)Para la topología presentada:
i.Indique las tablas de enrutamiento de los routers R1 y R2 de forma que permita conectividad extremo a extremo entre todos los equipos de la red.
ii.Indique las tablas de enrutamiento para los hosts de cada subred

b)Se sustituye el router R2 por un switch, al que se conectan todos los equipos de las subredes 2 y 3. Para lograr un nuevo esquema de numeración operativo, se desea modificar la menor cantidad de direcciones IP posibles.
i.Justifique la necesidad de renumerar alguna red para lograr una solución al problema.
ii.Represente gráficamente su solución con un esquema similar a de la figura anterior, indicando las nuevas direcciones IP para routers y hosts.
iii.Indique la tabla de enrutamiento del router R1 de forma que permita conectividad extremo a extremo entre todos los equipos de la red. Justifique las modificaciones realizadas.

Problema 2 (30 puntos)

Para realizar un ataque de tipo **TCP reset** que termine con una conexión establecida entre los hosts A y B, un tercer host C debe fabricar un paquete que tiene como dirección IP de origen la de A y como dirección IP destino la de B y, en su encabezado TCP tiene como puerto origen el que utiliza A en esa conexión TCP, como puerto destino el que utiliza B en ella, un número de secuencia válido (un entero de 32 bits) en la conexión activa entre A y B y el bit RST encendido. Cuando B recibe dicho paquete, inmediatamente corta la conexión con A. Como resultado tenemos un ataque de denegación de servicio (conocido como "DoS").
Para que este ataque funcione, alcanza con que el número de secuencia del paquete enviado por C sea válido dentro de la ventana en la que B esta esperando paquetes.

Dado que la ventanas de transmision tienen 16KBytes y que el paquete enviado por C no incluye carga útil, se pide:

a) Asumiendo conocidos los puertos y direcciones origen/destino de una conexión entre dos hosts A y B, calcule cuánto tiempo (análisis del "peor caso") se demora en tirar abajo una conexión establecida si disponemos de:

1. Bridge ADSL 512/128 Kbps (*notación:bajada/subida*)
2. Fast Ethernet (100 Mbps)

Justifique los valores numéricos utilizados en los cálculos, sin considerar overheads de capas 1 y 2 ni el tiempo que insume generar los paquetes y siendo despreciable el tiempo entre que se generan paquetes consecutivos. Se consideran conocidos puertos origen y destino, así como las direcciones IP origen y destino, siendo desconocido el número de secuencia.

b) Si queremos atacar un cliente de un servicio conocido (p.e. un browser), pero del que desconocemos el puerto utilizado en el cliente, calcule los tiempos máximos en tirar abajo la misma conexión si disponemos de:

1. Bridge ADSL 512/128 Kbps (*notación:bajada/subida*)
2. Fast Ethernet (100 Mbps)

Justifique los valores numéricos utilizados en los cálculos, sin considerar overheads de capas 1 y 2 ni el tiempo que insume generar los paquetes y siendo despreciable el tiempo entre que se generan paquetes consecutivos. Se consideran conocidos las direcciones IP origen y destino y también el puerto destino, siendo también desconocido el número de secuencia.

c) Cuando una aplicación realiza conexiones a un servidor, no se acostumbra especificar el puerto origen, dejándose esta tarea al sistema operativo. La mayoría de los sistemas operativos actuales los asignan en forma secuencial, tomando números dentro de un rango conocido. Sin embargo, BSD utiliza una estrategia de selección randómica de puertos. Discuta si este hecho nos permite afirmar que BSD es más seguro (o no) que otros sistemas operativos.

Problema 1 - Solución:

a)Para la topología presentada:
i.Indique las tablas de enrutamiento de los routers R1 y R2 de forma que permita conectividad extremo a extremo entre todos los equipos de la red.

Configuración Router R1

Network	Gateway	Interface
192.168.0.0/24	-	eth0
192.168.1.0/24	-	eth1
192.168.2.0/24	192.168.1.2	eth1

Configuración Router R2

Network	Gateway	Interface
192.168.2.0/24	-	eth1
192.168.1.0/24	-	eth0
192.168.0.0/24	192.168.1.1	eth0

ii.Indique las tablas de enrutamiento para los hosts de cada subred.

Cuando pedimos esto, se acepta que en un host pongan dos rutas, una a cada red, en lugar de tener solamente el default? Eso es algo que está bien, pero lo pregunto porque en el news lo preguntaron. Para mí se aceta y sin restar puntos.

Configuración hosts subred 1

Network	Gateway	Interface
192.168.0.0/24	-	eth0
0.0.0.0 def. gateway	192.168.0.1	eth0

Configuración hosts subred 2

Network	Gateway	Interface
192.168.1.0/24	-	eth0
0.0.0.0 def. gateway	192.168.1.1	eth0

Configuración hosts subred 3

Network	Gateway	Interface
192.168.2.0/24	-	eth0
0.0.0.0 def. gateway	192.168.2.1	eth0

a)Se sustituye el router R2 por un switch, al que se conectan todos los equipos de las subredes 2 y 3. Para lograr un nuevo esquema de numeración operativo, se desea modificar la menor cantidad de direcciones IP posibles.

i.Justifique la necesidad de renumerar alguna red para lograr una solución al problema.

Las direcciones IP consideradas para las subredes 1, 2 y 3 corresponden a redes contiguas.

Para agrupar direcciones se debe modificar la máscara de red, disminuyendo la cantidad de bits de la máscara, de modo que las redes incluidas sean comprendidas por la máscara utilizada.

Red	mascara	Redes /24 que la integran
192.168.0.0/23	11111111.11111111.11111110.00000000	192.168.0.0/24 192.168.0.1/24
192.168.2.0/23	11111111.11111111.11111110.00000000	192.168.0.2/24 192.168.0.3/24
192.168.2.0/22	11111111.11111111.11111100.00000000	192.168.0.0/24 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24

El problema que surge es que para incluir en una subred las subredes 192.168.1.0/24 y 192.168.2.0/24 se necesita una máscara /22 que incluye la red 192.168.0.0/24.

Por lo tanto la solución es renumerar tal que las subredes sean diferenciables por la máscara.

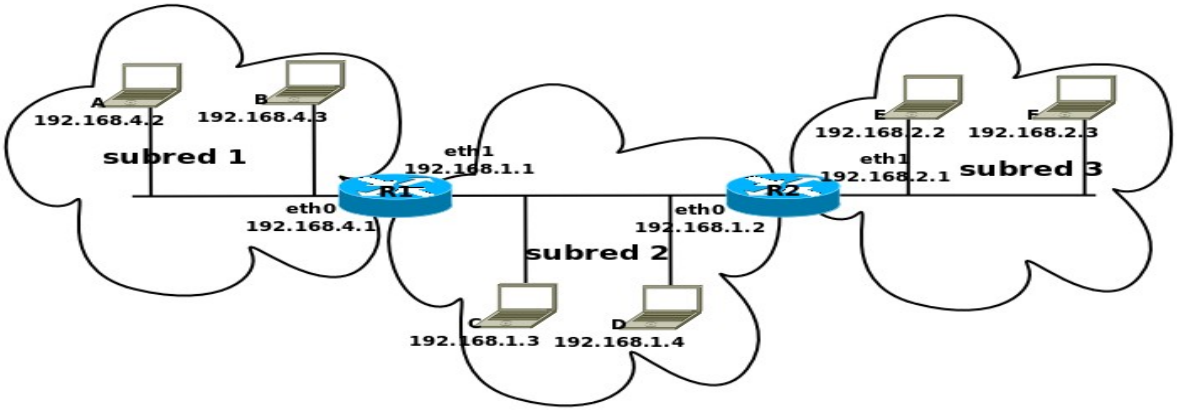
ii.Represente gráficamente su solución con un esquema similar a de la figura anterior, indicando las nuevas direcciones IP para routers y hosts.

Existen dos soluciones posibles, dejando contiguas las subredes 2 y 3 modificando únicamente una subred (dado que se pide modificar el menor número de direcciones IP).

Estas son:

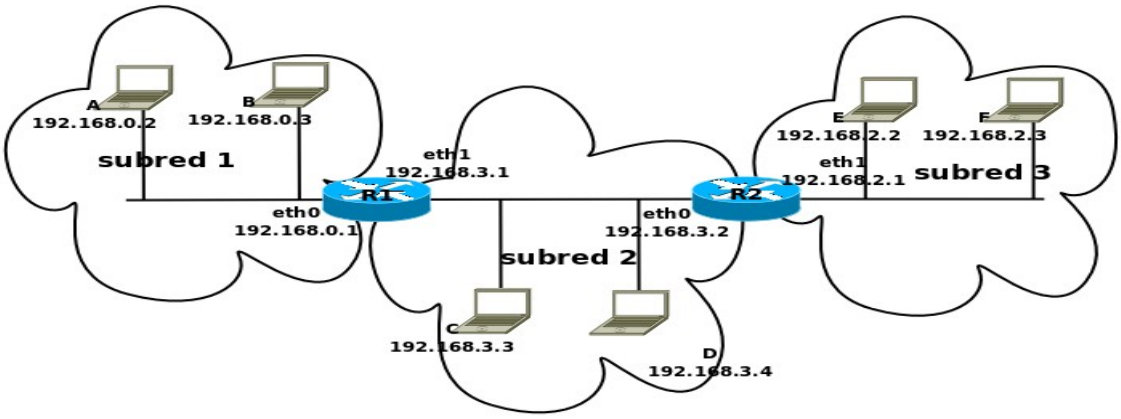
- modificar **subred 1** 192.168.0.0/24 a nueva subred192.168.4.0/24

Subred	máscara
Subred 1	192.168.4.0/24
Subred 2 y 3	192.168.0.0/22



- modificar **subred 2** 192.168.1.0/24 a nueva subred192.168.3.0/23

Subred	máscara
Subred 1	192.168.0.0/24
Subred 2 y 3	192.168.2.0/23



De las soluciones propuestas la primera es la ideal dado que modifica una IP menos. Por lo que es la que se considera para la parte iii.

iii.Indique la tabla de enrutamiento del router R1 de forma que permita conectividad extremo a extremo entre todos los equipos de la red. Justifique las modificaciones realizadas.

Configuración Router R1

Network	Gateway	Interface
192.168.4.0/24	-	eth0
192.168.0.0/22	-	eth1

Problema 2 - Solución:

a)
El ataque consistirá en enviar un mensaje válido, con el flag RST habilitado en el cabezal TCP para cada una de las ventanas posibles. Cada ventana tiene 16KB -> 2¹⁴bytes => $\frac{2^{32}}{2^{14}} = 2^{18}$ *ventanas cubren todo el rango de números de secuencias posibles. Por consiguiente, enviando 2¹⁸ paquetes, ensamblados como describe la letra y con el RST activado, con números de secuencia tales que uno pertenezca a cada ventana, vamos a poder cortar una conexión establecida .*

Cabezal IP (sin opciones) : 20 bytes
Cabezal TCP (sin datos) : 20 bytes => cada mensaje a enviar tiene 40 bytes, 320 bits.

La totalidad del ataque requiere 2¹⁸ x 320 bits en total, del órden de 80 millones de bits.

a.1) Si contamos con una conexión ADSL, debemos considerar la tasa de transmisión o uplink, que es de 128.000 bits por segundo. Transmitir esos 80.000.000 de bits a 128.000 bits por segundo tomaría
$\frac{80000000}{128000 s^{-1}} = 80000/128 s^{-1} = 625 s$
a.2) Con una conexión FastEthernet, capaz de transmitir en bruto 100.000.000bps, si obviamos los overheads de capa 1 y 2 y los tiempos involucrados en la generación de los paquetes, tenemos que en menos de un segundo podríamos transmitir la totalidad del ataque.
a.3) Con una conexión Gigabit Ethernet, podríamos transmitir la totalidad del ataque en una décima de segundo, aproximadamente, obviando la capacidad de procesamiento el equipo atacante ylos overheads de capa 1 y 2.

b)
Dado que desconocemos el puerto utilizado por el cliente para la conexión, deberíamos probar, en el peor caso, a cada uno de los 2¹⁶ puertos posibles.
b.1) 625x65536 segundos, del órden de los 475 días, algo menos de 2 años.
b.2) Si asumimos que el ataque podía realizarse en aproximadamente 1 segundo para un puerto, los 65536 puertos pueden se probados en 65536 segundos, algo más de 18hs.
b.3) Si asumimos que el ataque podía realizarse en aproximadamente una décima de segundo para un puerto, entonces, los 65536 puertos pueden ser probados en 6554 segundos, algo menos de 2hs.

<u>Adicional:</u> De conocer algún dato más sobre la aplicación atacada y el sistema operativo destino quizás podríamos ajustar la búsqueda a un rango menor de puertos, pero presentamos el análisis del peor caso. Dependiendo del tipo de aplicación, probablemente no utilice puertos privilegiados (eliminando 1024 pruebas). También es posible acotarlas a ciertos rangos dependiendo del sistema operativo.

c)
Para un análisis del tipo worst-case, como el realizado, la selección randómica de puertos no nos podría ayudar a reducir el espacio de búsqueda. De todas formas, en la vida real, el no disponer de estas estrategias podrían facilitar a un atacante el trabajo. Por ejemplo, si es conocido el número desde el que comienza la asignación secuencial de puertos, los sistemas serían más fácilmente atacables inmediatamente luego de encendidos. Otra riesgo asociado a la asignación secuencial de puertos orígenes de conexiones es que, si un atacante descubre un puerto asignado, tiene entonces la posibilidad de reducir el tiempo necesario para encontrar el puerto a atacar.
Si bien este es un riesgo inherente a TCP y no es eliminado en base a la randomización de puertos para un análisis del peor caso, desde el punto de vista práctico elimina la forma de poder fácilmente reducir el rango de puertos a atacar.