INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ÁNDRES TUXTLA
INGENIERÍA INFORMATICA
MATERIA: SISTEMAS OPERATIVOS
EVIDENCIAS UNIDAD 4

INVESTIGACION 30% LISTA DE COTEJO

NOMBRE DEL DOCENTE: María de los Ángeles Pelayo Vaquero	FIRMA DEL DOCENTE

DATOS GENERALES DEL PROCESO DE EVALUACIÓN			
NOMBRE DEL ALUMNO: BLAS DIAZ ABISAI			GRUPO 510-A
PRODUCTO: Investigación	UNIDAD: 4	FECHA 05-DIC- 2023	PERIODO ESCOLAR: SEPTIEMBRE 2023 – ENERO 2024

INDICADOR	VALOR	PORCENTAJE OBTENIDO
Presentación - Formato	5	5
Introducción Idea clara del contenido del trabajo, motivando al lector a continuar con su lectura y revisión	5	5
Desarrolla el objetivo	5	5
Desarrollo de la investigación La investigación cumple con el tema solicitado	5	5
Desarrolla la conclusión de investigación	5	5
Gramática y ortografía	2	5
Bibliografía	3	2
Total	**30%**	30%

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ÁNDRES TUXTLA
INGENIERÍA INFORMATICA
MATERIA: SISTEMAS OPERATIVOS
EVIDENCIAS UNIDAD 4

LISTA DE COTEJO REPORTE DE PRACTICA 30%

NOMBRE DEL DOCENTE: María de los Ángeles Pelayo Vaquero			FIRMA DEL DOCENTE
DATOS GENERALES DEL PROCESO DE EVALUACIÓN			
NOMBRE DEL ALUMNO: BLAS DIAZ ABISAI			
PRODUCTO: REPORTE DE PRACTICA	UNIDAD: 4	FECHA 13-DIC- 2023	PERIODO ESCOLAR: SEPTIEMBRE 2023 – ENERO 2024

RUBRICAS	Porcentaje %	Puntos
Selecciona sistemas operativos basados en Linux para las practicas	2	2
Identifica los requerimientos de los sistemas operativos	2	2
Desarrolló y explicó el proceso de configuración de la tarjeta de red en sistemas operativos virtualizados basados en Linux	10	10
Configura la maquina anfitrión para compartir carpeta, usa comandos básicos o entorno grafico	10	10
Identificó la funcionalidad de los principales comandos para configurar servidor	4	4
Mostro el funcionamiento de las práctica relacionado con el objetivo	2	2
Total	30 %	30 %

ANEXOS

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

CARRERA:

Ingeniería Informática

GRUPO:

510-A

ASIGNATURA:

Sistemas Operativos II

CATEDRÁTICO:

M.T.I. Maria De Los Angeles Pelayo Vaquero

ALUMNO:

Abisai Blas Díaz

FECHA:

4/12/2023

SAN ANDRES TUXTLA VER

INTRODUCCIÓN

Como introducción veremos el tema la conexión dinámica es un método de comunicación entre dos o más dispositivos que permite establecer y terminar la conexión según la demanda este método tiene ventajas como la flexibilidad, la eficiencia y la seguridad, pero también implica algunos desafíos como la complejidad, la latencia y el control de errores. En este texto, se explicará el concepto de conexión dinámica, sus características, sus aplicaciones y sus desafíos. La arquitectura cliente-servidor es un modelo de diseño de software que permite la comunicación entre dos o más procesos distribuidos en una red. En este modelo, un proceso llamado cliente solicita un servicio a otro proceso llamado servidor, que lo provee. El cliente y el servidor pueden ejecutarse en la misma máquina o en máquinas diferentes, y pueden comunicarse mediante diversos protocolos de red. La tolerancia a fallos es la capacidad de un sistema operativo para continuar funcionando correctamente en caso de que ocurra algún error o falla en alguno de sus componentes. La tolerancia a fallos implica el uso de técnicas de detección, corrección y recuperación de errores, así como la redundancia de hardware y software. El objetivo de la tolerancia a fallos es garantizar la disponibilidad, fiabilidad y seguridad de los sistemas operativos.

CONEXIÓN DINAMICA, CLIENTE-SERVIDOR Y TOLERANCIA A FALLOS SISTEMAS OPERATIVOS.

La conexión dinámica es un método en integrar dentro del código del cliente la dirección en la red del servidor. El problema de este método es que es muy rígido si el servidor se desplaza se duplica o si cambia la interfaz, habría que localizar y volver a compilar numerosos programas para asi evitar todos esos problema, ciertos sistemas distribuidos utilizan lo que esta sección como las ideas de la conexión dinámica.

Sin embargo, esta forma de conexión dinámica también tiene sus desventajas existe un costo adicional en el tiempo generado por la exportación e importación de las interfaces puesto que muchos procesos clientes tienen vida corta y cada proceso tiene que comenzar de nuevo el efecto puede ser significativo.

Semántica de rcp en presencia de fallas el objetivo de este es ocultar la comunicación al hacer que las llamadas a procedimientos remotos se parezcan a las locales. En tanto si como el cliente como el servidor funcionan de manera perfecta rpc hace su trabajo en forma excelente hay cinco clases para distintas fallas en rcp que el cliente no puede localiza al servidor, se pierde el mensaje de solicitud del cliente al servidor, el servidor falla antes de recibir una solicitud y por ultimo el cliente falla después de enviar una solicitud.

Pérdida de mensaje de solicitud este es más fácil de tratar lo único que hay que hacer es que el núcleo inicie un cronómetro al enviar la solicitud si el tiempo se termina antes de que regrese una respuesta a reconocimiento el núcleo vuelve a enviar el mensaje. Si mensaje en realidad se perdió el servidor no notará la diferencia entre la retransmisión y el original y todo funcionará bien. Perdida de mensajes de respuesta la pérdida de respuestas más fácil de enfrentar las solución obvia es basarse De nuevo a un cronómetro si no llega una respuesta en el periodo razonable sólo hay que enviar de nuevo la solicitud el problema con esta solución es que el núcleo Del cliente no está seguro de la razón por la que hubo respuesta.

Tolerancia a fallas es la capacidad de un sistema de seguir funcionando correctamente en presencia de fallos o errores en algunos de sus componentes. Un sistema tolerante a fallas puede detectar, aislar y recuperarse de los fallos, minimizando así el impacto en el rendimiento, la disponibilidad y la seguridad del sistema la tolerancia a fallas se logra mediante el uso de técnicas de redundancia, diversidad, monitorización y auto reparación, entre otras.

Fallas de componentes pueden fallar debido a una falla de algún componente como procesador, la memoria asi como cable o el software, las fallas se clasifican por lo general como transitorias, intermitentes o permanentes la fallas transitorias ocurren una vez y después desaparecen si la operación se repite, si ocurre una falla intermitente ocurren una vez y después se desaparecen, si la operación se repite la falla ya no se presenta. Una falla permanente es aquella que continúa existiendo hasta reparar el componente con el desperfecto.

Fallas de sistemas con frecuencia puede sobrevivir a las fallas de los componentes en vez de hacer en un sistema sea poco probables, la confiabilidad de un sistema en particular importante en un sistema distribuido.

Tolerancia de fallas mediante respaldo primario es el respaldo ocupa su lugar el reemplazo debe ocurrir de manera limpia y ser notado únicamente por el sistema operativo cliente, la tolerancia de fallas con respaldo primario tiene dos ventajas principales sobre la réplica activa en primer lugar es mas sencilla durante la operación normal puesto que los mensajes van solo a un servidor primario y no a todo un grupo. Como desventaja trabaja mal en presencia de fallas bizantinas en las que el primario afirma erróneamente que funciona de manera perfecta, además la recuperación de una falla del primario puede ser compleja y consumir mucho tiempo.

La tolerancia a fallas mediante respaldo primario es una técnica que permite a un sistema informático continuar funcionando en caso de que uno de sus componentes falle.

Consiste en tener un componente principal que realiza las tareas del sistema y uno o más componentes de respaldo que están listos para asumir el control si el principal falla el componente principal envía periódicamente señales de vida al componente de respaldo para indicar que está operativo. Si el componente de respaldo no recibe una señal de vida en un tiempo determinado, asume que el principal ha fallado y toma el control del sistema. De esta manera, se minimiza el tiempo de inactividad y se garantiza la disponibilidad del servicio.

CONCLUSIÓN

En conclusión, de conexión dinámica es un proceso que permite a los dispositivos de red establecer y terminar conexiones de forma automática y flexible. Este proceso facilita la gestión de la red, reduce el consumo de recursos y mejora la seguridad y el rendimiento. La conclusión de conexión dinámica se basa en protocolos como DHCP, NAT, VPN y otros que asignan direcciones IP, puertos, identificadores y claves a los dispositivos de forma temporal y según la demanda.

En conclusión, cliente-servidor es un modelo de comunicación que permite la interacción entre dos o más entidades en una red. El cliente es el que solicita un servicio o recurso al servidor, que es el que lo provee o lo gestiona. Este modelo tiene varias ventajas, como la distribución de la carga de trabajo, la escalabilidad, la modularidad y la seguridad. Sin embargo, también presenta algunos desafíos, como la dependencia del servidor, la latencia, la sincronización y la complejidad.

Como conclusión la tolerancia a fallas es la capacidad de un sistema de seguir funcionando correctamente en presencia de fallas parciales. Esta característica es esencial para garantizar la fiabilidad, la disponibilidad y la seguridad de los sistemas críticos. La tolerancia a fallas se logra mediante el uso de técnicas de redundancia, detección y recuperación de errores, y aislamiento y contención de fallas.

REPORTE DE PRACTICA SUBIR EN PDF

NOMBRE DE LOS INTEGRANTES DE EQUIPO

NOMBRE (s)	**APELLIDOS**
ABDIEL MIGUEL	GOMEZ ALEMAN
YAHIR	CAMPOS MARTINEZ
ABISAI	BLAS DIAZ
LUIS ENRIQUE	RIVAS CHAMPALA
EDDI JOSUE	ZUÑIGA CHAVEZ

Integracion de practicas

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

INGENIERÍA INFORMÁTICA

MATERIA:

SISTEMAS OPERATIVOS II

TEMA:

REPORTE DE PRACTICAS

ALUMNOS:

ABDIEL MIGUEL GOMEZ ALEMAN

YAHIR CAMPOS MARTINEZ

ABISAI BLAS DIAZ

LUIS ENRIQUE RIVAS CHAMPALA

EDDI JOSUE ZUÑIGA CHAVEZ

QUINTO SEMESTRE

GRUPO 510-A

DOCENTE:

MTI. MARIA DE LOS ANGELES PELAYO VAQUERO

8 DE DICIEMBRE DE 2023

ÍNDICE DE CONTENIDO

PRACTICA 1. SERVIDOR DHCP

Introducción

El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como Dynamic Host Configuration Protocol, es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados.

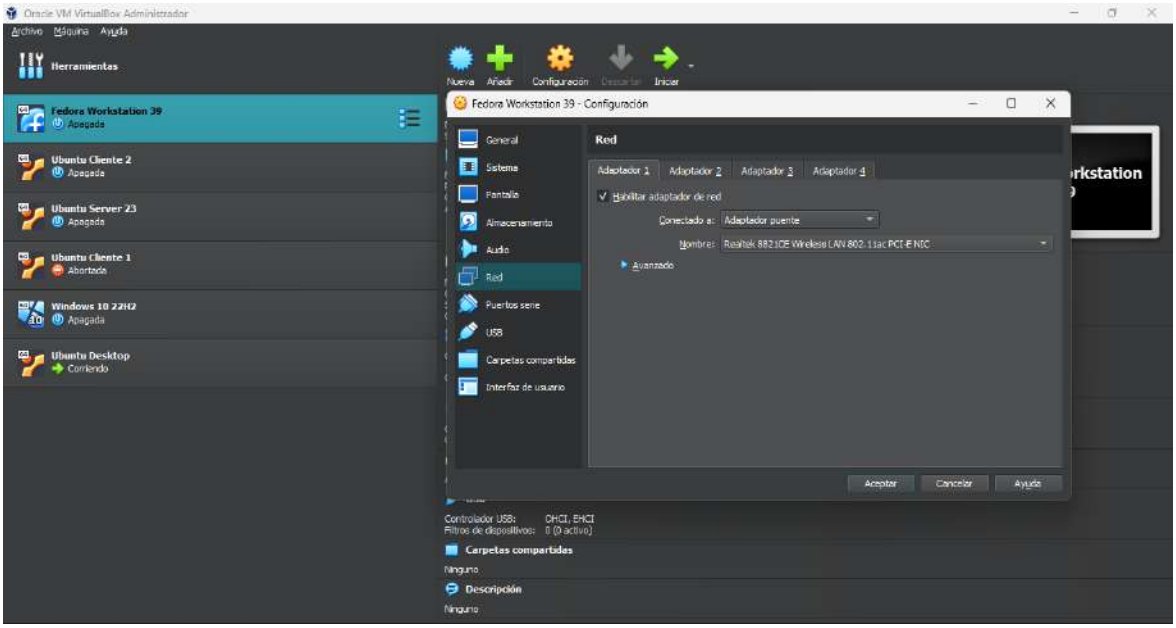
Este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión. También el servidor DHCP asigna dinámicamente la máscara de subred, los gateways predeterminados y otros parámetros de la red que solicitan los dispositivos.

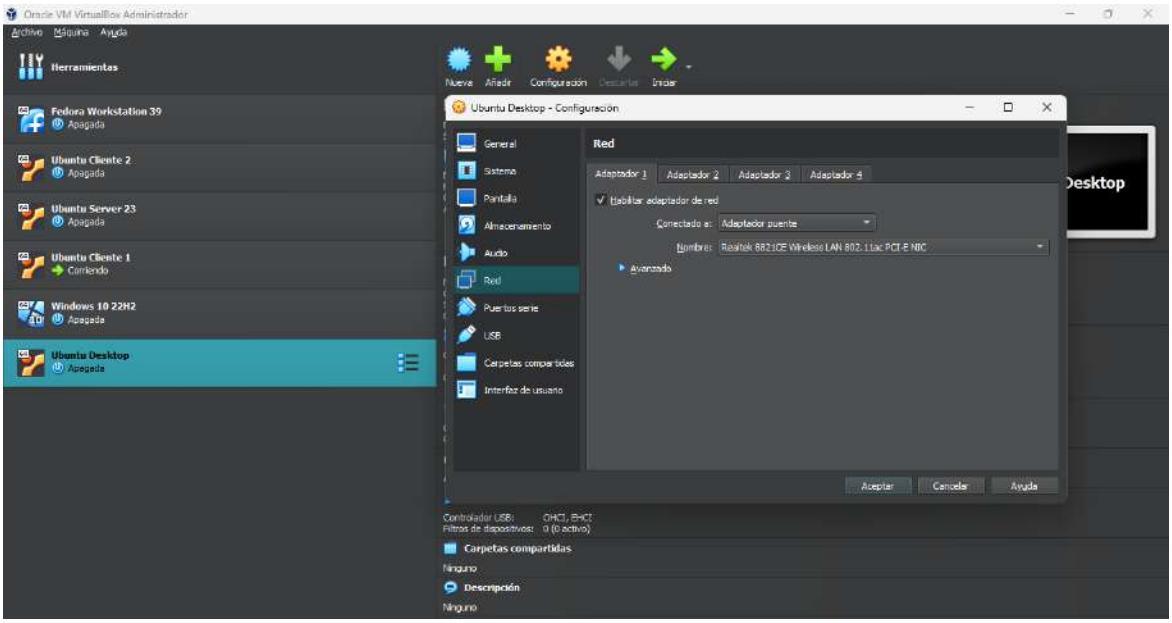
Objetivo

El objetivo principal de esta práctica es familiarizarse con la configuración y operación de un servidor DHCP virtual, así como la configuración y conexión de máquinas virtuales y físicas en un entorno de virtualización. Los pasos que seguir incluyen la configuración del servidor DHCP en Fedora, la configuración de máquinas virtuales/físicas como clientes, y la verificación de la asignación de direcciones IP dinámicas a través del protocolo DHCP.

Configuración y demostración

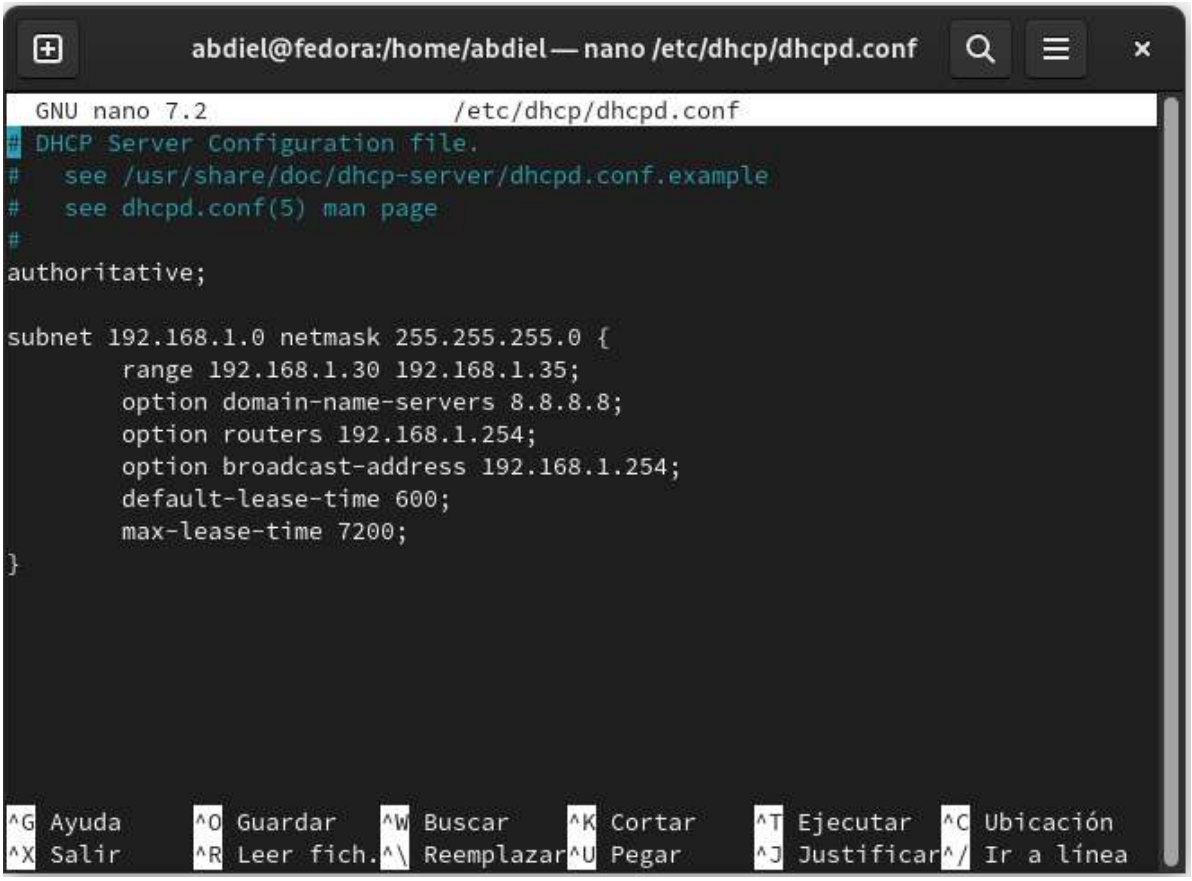
En esta práctica se utiliza un router físico para crear conexión en WLAN. Se usa el software Oracle VM VirtualBox para virtualizar las maquinas que se designarán como servidor y clientes. Antes de iniciar la máquina virtual Fedora 39 (Servidor) y las máquinas virtuales (clientes), se selecciona en configuración de red “Red puente” y se elige el nombre del adaptador de red que usa la maquina física.



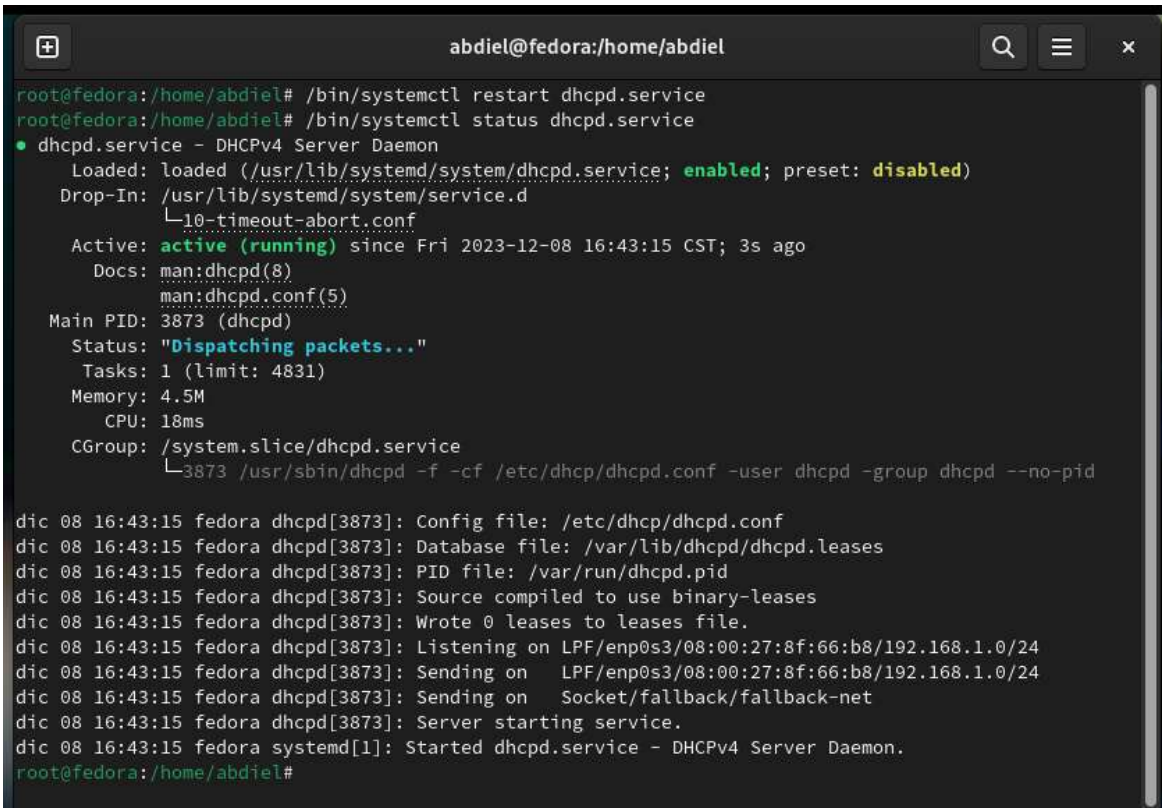


Para instalar y configurar el servidor DHCP, en la terminal Fedora 39 se inicia sesión con contraseña root mediante el comando "**su**" y se ejecuta el comando "**dnf -y install dhcp-server**" para instalar el servidor. Se edita el fichero de configuración del servidor DHCP con "**nano /etc/dhcp/dhcpd.conf**".

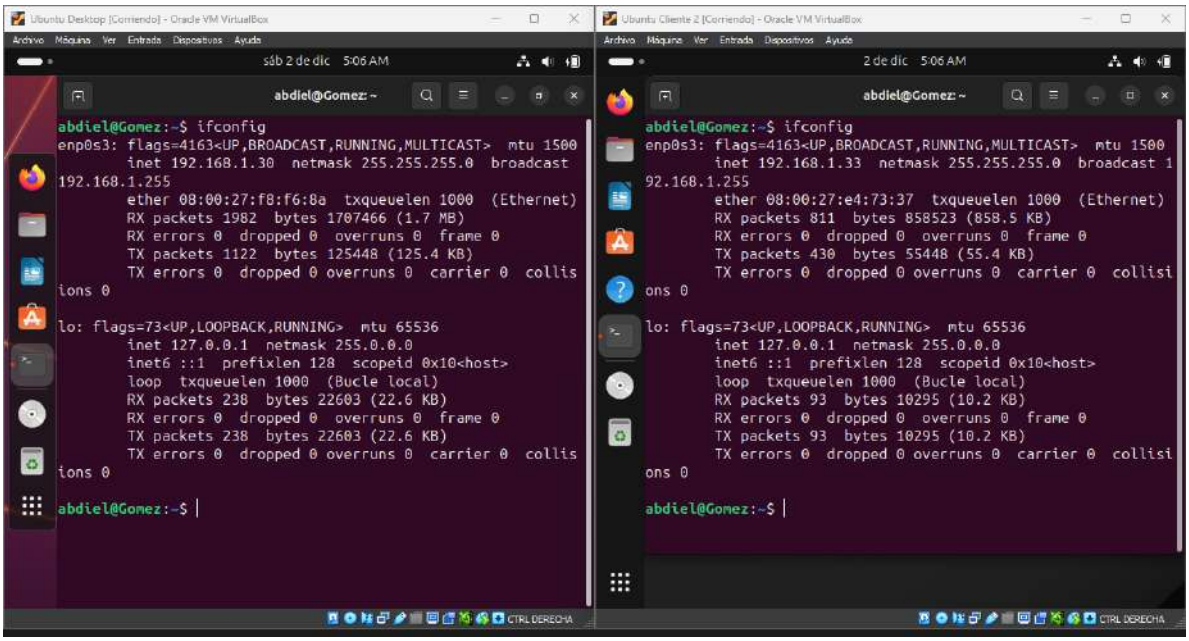
Este archivo permite asignar direcciones IP de un rango dado, en este caso de la 30 a la 35, en él, se especifican parámetros, como la IP del servidor, la dirección de la red, la submáscara, la dirección de broadcast, entre otros.



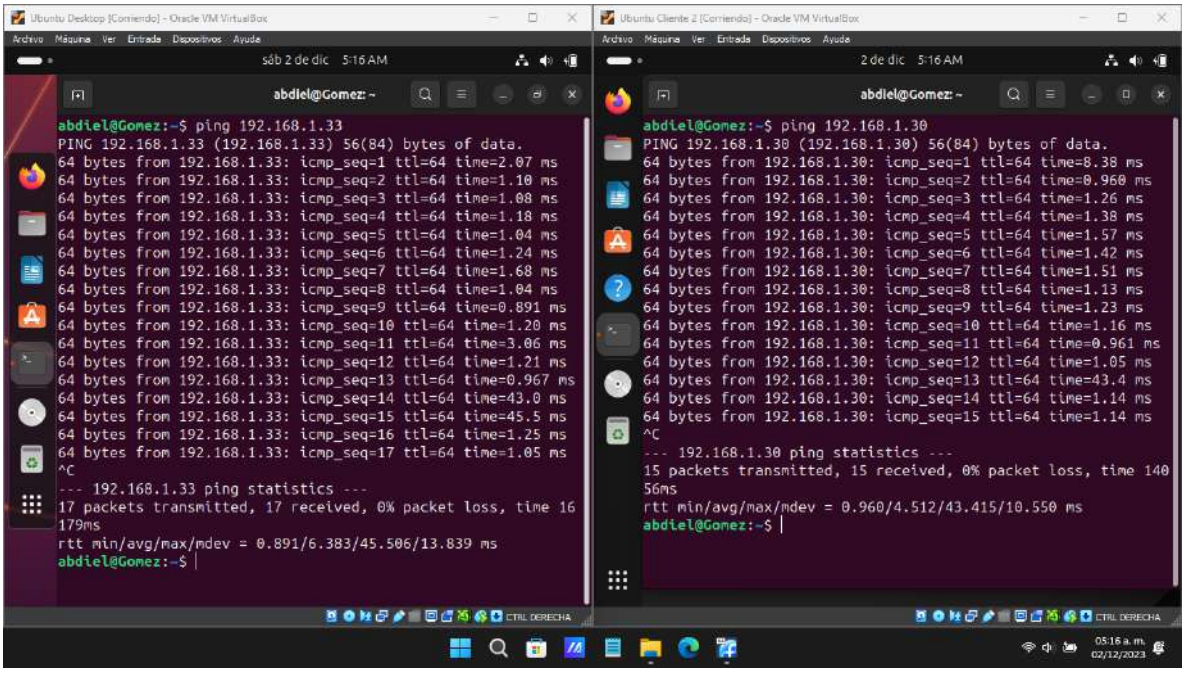
Una vez finalizada la configuración del archivo anterior, debemos reiniciar el servicio. Utilizaremos el comando "**/bin/systemctl restart dhcpd.service**" para reiniciar el servicio, "**/bin/systemctl status dhcpd.service**" para comprobar el estado de nuestro servidor DHCP, "**/bin/systemctl stop dhcpd.service**" para parar el servicio, y "**/bin/systemctl start dhcpd.service**" para iniciar el servicio.



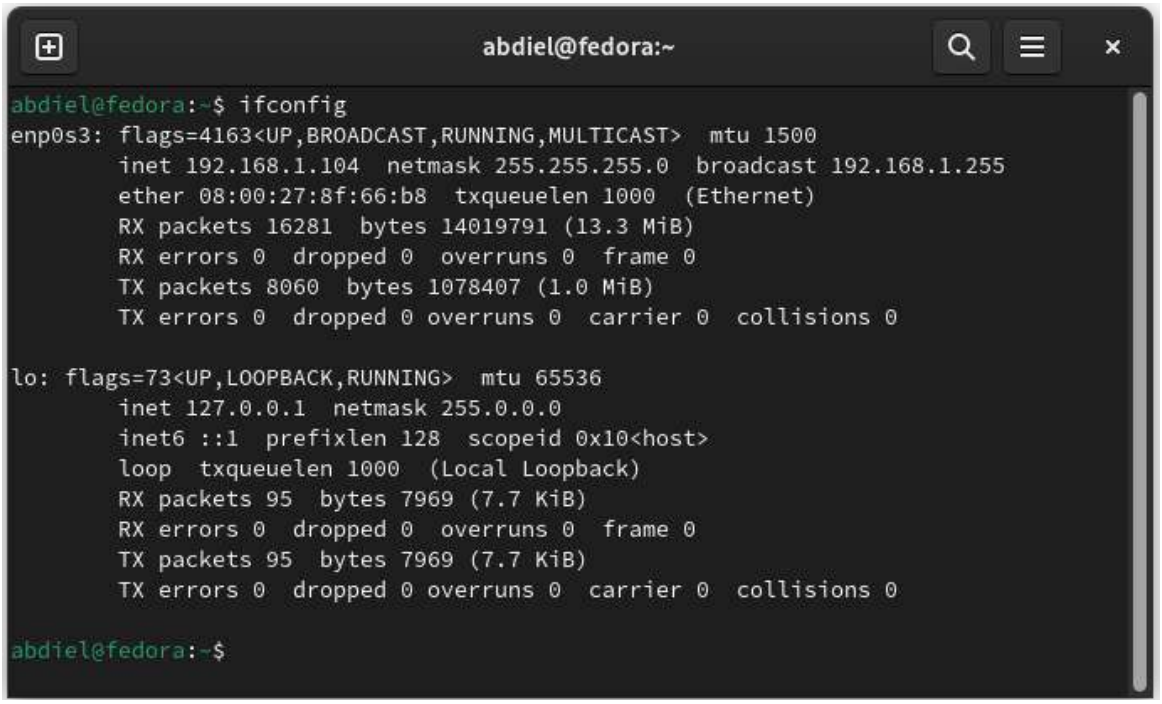
Se conectan las máquinas virtuales de Ubuntu con el cliente DHCP y se hace un "**ifconfig**" para verificar que el servidor les asignó las IPs establecida en el rango.

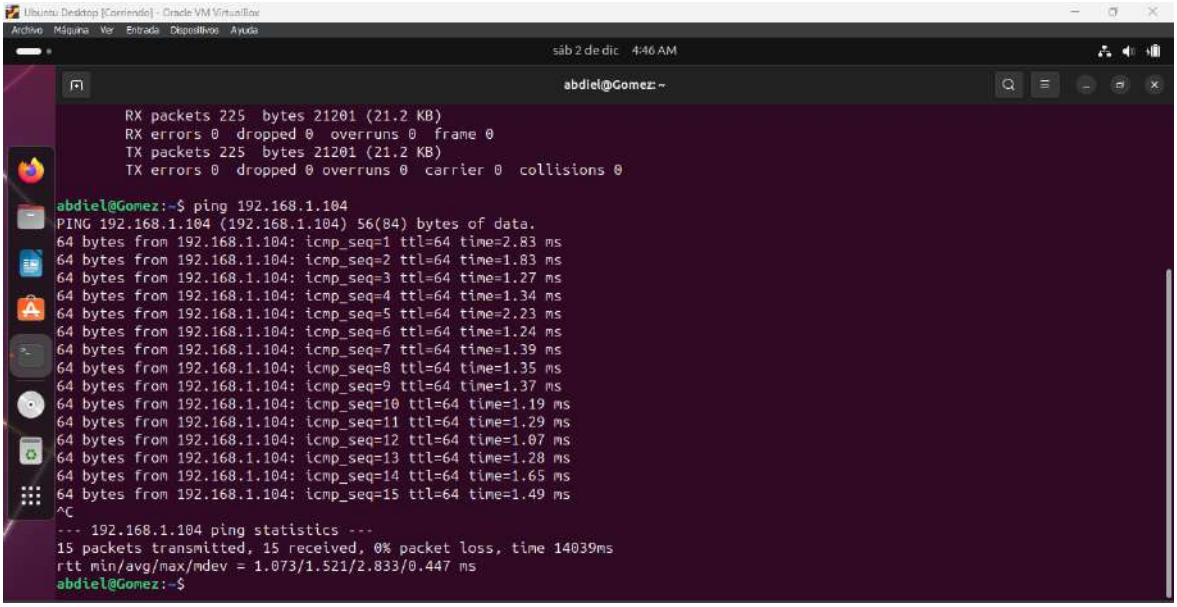


Se hace ping entre las maquinas clientes:

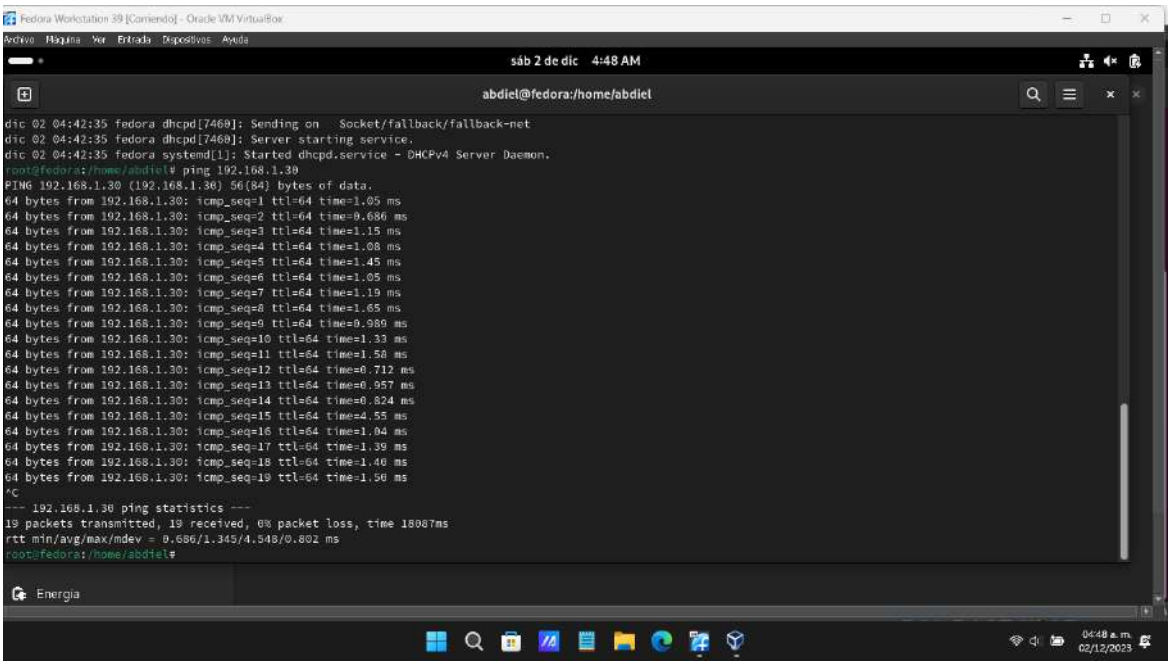


La máquina cliente Ubuntu Desktop hace ping con el Servidor DHCP Fedora (IP 192.168.1.104).



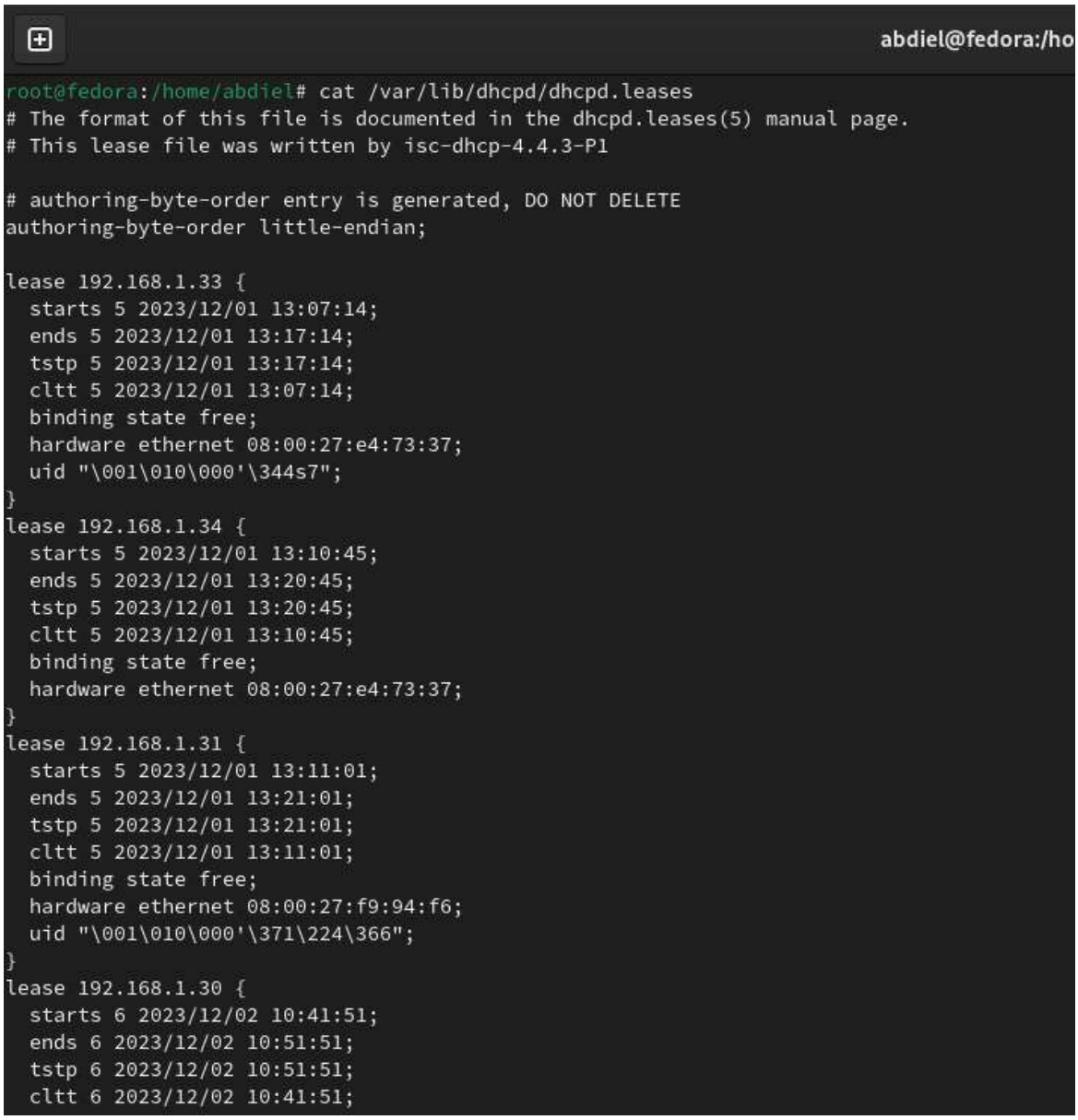


El servidor DHCP hace ping con la maquina cliente Ubuntu Desktop:



En linux sí un cliente no tiene asignada la IP del rango del servidor DHCP, se ejecuta "**sudo dhclient -r**" para soltar la IP actual y con "**sudo dhclient -4**" tomaría otra IP que debe estar dentro del rango establecido en la configuración del archivo del servidor.

El archivo de arrendamiento es proporcionado por el servidor DHCP y contiene toda la información de arrendamiento sobre cada cliente que ha obtenido una dirección IP del servidor. Cuando tiene un cliente que tiene una dirección DHCP, se puede ver el archivo de arrendamientos utilizando el comando: **“cat /var/lib/dhcpd/dhcpd.leases**”



Uso y aplicación

El Protocolo de Configuración Dinámica de Hosts (DHCP) es fundamental en redes informáticas para simplificar la administración y configuración de direcciones IP en dispositivos. Aquí se describen algunos de los usos y aplicaciones clave de los servidores DHCP:

1. **Asignación Automática de Direcciones IP:** El principal propósito de un servidor DHCP es asignar direcciones IP automáticamente a dispositivos en una red. Cuando un dispositivo se conecta a la red, el servidor DHCP le asigna una dirección IP disponible, lo que elimina la necesidad de configurar manualmente cada dispositivo en la red.
2. **Configuración de Otros Parámetros de Red:** Además de las direcciones IP, DHCP puede proporcionar información adicional de configuración de red, como la máscara de subred, la puerta de enlace predeterminada, los servidores DNS y los servidores WINS. Esto simplifica aún más la configuración de los dispositivos en la red.
3. **Eficiencia en la Administración de IP:** En entornos grandes, la administración manual de direcciones IP puede volverse engorrosa y propensa a errores. DHCP automatiza este proceso, garantizando que las direcciones IP se asignen de manera eficiente y evitando conflictos de direcciones.
4. **Migración y Cambios de Dispositivos:** Cuando se realizan cambios en la red, como la adición de nuevos dispositivos o la migración de dispositivos de un segmento de red a otro, DHCP facilita la actualización de las configuraciones de red sin necesidad de intervención manual.
5. **Ahorro de Direcciones IP:** DHCP puede ser configurado para asignar direcciones IP de manera temporal (por tiempo limitado). Esto permite reutilizar direcciones IP que ya no están en uso, optimizando el uso de direcciones en la red.
6. **Facilita la Implementación de Redes Temporales o en Eventos:** En situaciones temporales, como eventos o configuraciones provisionales,

DHCP facilita la implementación rápida de una red sin requerir una configuración manual detallada.

7. **Reducción de Errores de Configuración:** Al automatizar la asignación de direcciones IP y la configuración de red, se reducen los errores humanos, ya que se minimiza la posibilidad de configuraciones incorrectas o conflictos de direcciones.
8. **Auditoría y Registro de Actividades:** Muchos servidores DHCP tienen capacidades de registro que permiten la auditoría de las asignaciones de direcciones IP. Esto es útil para realizar un seguimiento de la actividad de la red y solucionar problemas.

PRACTICA 2. SERVIDOR DNS

Introducción

DNS es un servicio estándar del sector que se usa para localizar equipos en una red basada en protocolo de Internet (IP). Los usuarios de red se basan en nombres basados en caracteres, como www.microsoft.com. Por lo tanto, es necesario traducir caracteres o direcciones fáciles de usar en las direcciones basadas en números (207.46.131.137) que la red puede reconocer. DNS es el servicio que se elige para buscar recursos y traducirlos a sus direcciones IP correspondientes.

DNS usa una base de datos especializada de registros de recursos, que normalmente se conoce simplemente como RR, para responder a las consultas de resolución de nombres de cliente. Antes de DNS, la resolución de nombres en Internet se lograba con el “archivo de hosts” (Un archivo creado manualmente que reside en un host que asocia nombres de host con direcciones IP), que se crean manualmente archivos que asocian nombres de host con direcciones IP.

Cuando se agregó un nuevo cliente a la red, un administrador tenía que actualizar manualmente el archivo de hosts y, a continuación, copiar (replicar) ese archivo en todos los demás equipos de la red para que todos pudieran llegar al nuevo host. A medida que internet creció, esta forma de resolución de nombres era claramente insuficiente; era demasiado intensivo en la administración, y no se escalaba. El archivo de hosts acaba de ser más grande y porque usó un espacio de nombres plano (vea también Espacio de nombres), no se pudo crear particiones y tuvo que distribuirse en su totalidad. La solución era DNS.

Por ejemplo, en el dominio ficticio widgets.products.microsoft.com, la responsabilidad de la resolución de nombres se puede particionar para que varios servidores puedan controlar la resolución de nombres para diferentes partes del espacio de nombres:

EVALUACION UNIDAD 4. SISTEMAS OPERATIVOS 2

VALOR: 35%

INGENIERÍA INFORMÁTICA ITSSAT

Se ha registrado el correo del encuestado (**211u0367@alumno.itssat.edu.mx**) al enviar este formulario.

NOMBRE Y APELLIDOS *

ABISAI BLAS DIAZ

GRUPO: *

510-A

Se distinguen entre cinco clases distintas de fallas que pueden ocurrir en los sistemas RPC: * 5 puntos

1. El cliente no puede localizar al servidor.

2. Se pierde el mensaje de solicitud del cliente al servidor.

3. Se pierde el mensaje de respuesta del servidor al cliente.

4. El servidor falla antes de recibir una solicitud.

5. El cliente falla después de enviar una solicitud.

Cada una de estas categorías tiene distintos problemas y necesita distintas soluciones

- ( ) F
- (•) V

Pérdida de mensajes de solicitud: lo único que hay que hacer es que el núcleo inicie un cronómetro al enviar la solicitud. Si el tiempo se termina antes de que regrese una respuesta o reconocimiento, el núcleo vuelve a enviar el mensaje. Si el mensaje en realidad se perdió, el servidor no notará la diferencia entre la retransmisión y el original y todo funcionará bien. A menos, por supuesto, que se pierdan tantos mensajes que el núcleo se dé por vencido y concluya erróneamente que el servidor está inactivo, en cuyo caso regresamos al caso "no se pudo localizar al servidor". * 5 puntos

- (•) V
- ( ) F

Fallas del cliente: ¿Qué ocurre si un cliente envía una solicitud a un servidor para que se realice cierto trabajo y falla antes de que el servidor responda? En este momento, está activa una labor de cómputo y ningún padre espera el resultado. Esta labor de cómputo no deseado se llama huérfano. * 5 puntos

Los huérfanos provocan varios problemas. Como mínimo, desperdician los ciclos del CPU. Bloquean archivos o capturan recursos valiosos. Por último, si el cliente vuelve a arrancar y realiza de nuevo la RPC, pero la respuesta del huérfano regresa de inmediato, puede surgir una confusión.

- ○ F
- ◉ V

Fallas de sistema: En un sistema distribuido crítico, con frecuencia nos interesa que el ***sistema*** pueda sobrevivir a las fallas de los componentes (en particular, del procesador), en vez de hacer que las fallas sean poco probables. La confiabilidad de un sistema es en particular importante en un sistema distribuido, debido a la gran cantidad de componentes presentes; de ahí la mayor posibilidad de que falle uno de ellos. * 5 puntos

- ◉ V
- ○ F

Con las fallas salientes, un procesador que falla sólo se detiene y no responde a las entradas subsecuentes ni produce más entradas, excepto que puede anunciar que ya no está funcionando. También se llaman fallas de detención. * 5 puntos

- ◉ F
- ○ V

Si un procesador puede enviar un mensaje y sabe que la ausencia de respuesta dentro de T segundos significa que el pretendido receptor ha fallado, puede realizar una acción correctiva. Si no existe una cota superior para el tiempo de la respuesta, será un problema determinar incluso si ha ocurrido una falla. * 5 puntos

- (●) V
- ( ) F

La tolerancia de fallas en general y la réplica activa en particular, en muchos sistemas, los servidores actúan como grandes máquinas de estado finito: aceptan solicitudes y producen respuestas. La lectura de solicitudes no altera el estado del servidor, pero la escritura de solicitudes sí lo hace. Si cada solicitud cliente se envía a cada servidor y todas son recibidas y procesadas en el mismo orden, entonces, después de procesar cada una, todos los servidores que no han fallado tendrán con exactitud el mismo estado y darán las mismas respuestas. El cliente o votante puede combinar todos los resultados para enmascarar las fallas. * 5 puntos

- (●) V
- ( ) F

La tolerancia de fallas con respaldo primario tiene dos ventajas principales sobre la réplica activa. En primer lugar, es más sencilla durante la operación normal, puesto que los mensajes van sólo a un servidor (el primario) y no a todo un grupo. Los problemas asociados con el ordenamiento de estos mensajes también desaparecen. En segundo lugar, en la práctica se requieren menos máquinas, puesto que en cualquier instante se necesitan un primario y un respaldo (aunque cuando un respaldo se pone en servicio como primario, se necesita un nuevo respaldo de manera instantánea).

* 5 puntos

- ○ F
- ◉ V